



Joni Sirkiä

Murtautumistestauksen harjoittelun soveltuvuus tietoturvallisuustietoisuuden lisäämiseksi

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikan tutkinto-ohjelma

Insinööriyö

30.10.2024

Tiivistelmä

Tekijä:	Joni Sirkiä
Otsikko:	Murtautumistestauksen harjoittelun soveltuvuus tietotur- vallisuuksiin lisäämiseksi
Sivumäärä:	59 sivua + 2 liitettä
Aika:	30.10.2024
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikan tutkinto-ohjelma
Ammatillinen pääaine:	Tietojenkäsittely ja tietoliikenne
Ohjaajat:	Osaamisaluejohtaja Janne Salonen

Verkkorikollisuudelle alttiit internetiin kytketyt tietojärjestelmät ja tietoaaineistot ovat entistä kiinteämmin osa jokapäiväistä elämäämme, mikä altistaa meidät merkittäville tietoturvariskeille. Yksi oleellisimmista vastatoimista tietoturvariskejä vastaan on tietoturvatietoisuuden lisääminen. Tietoturvatietoisuuden lisäämiseksi on olemassa useita menetelmiä, joilla on omat haasteensa ja rajoitteensa. Tämän työn tarkoitus oli tutkia yhtä mahdollista koulutusmenetelmää, pelillistä murtautumistestauksen harjoittelua, tavoitteena selvittää, miten murtautumistestauksen harjoittelu soveltuu tietoturvatietoisuuden lisäämiseksi.

Tämä tutkimus toteutettiin osin kirjallisuustutkimuksena ja osin laadullisena kokemuk-
siin perustuvana reflektioivana tutkimuksena, jonka tuloksia vertailtiin tekoälyavuste-
isiin vertailututkimukseen. Kirjallisuustutkimuksella koottiin tutkimuksen teoreettinen
viitekehys, sekä yleinen katsaus murtautumistestauksen roolista osana tietoturvalli-
suutta. Laadullisella tutkimuksella tutkittiin kuinka pelillistetty murtautumistestauksen
harjoittelu voi vaikuttaa tietoturvatietoisuuteen, sekä tietoturvallisuuteen yleisesti.
Laadullinen tutkimus tehtiin reflektioivalla tutkijan omia kokemuksia murtautumistes-
tauksen harjoittelusta TryHackMe-alustalla, sekä vertailemalla näitä kokemuksia mui-
den käyttäjien kokemuksiin. Muiden käyttäjien kokemukset kasattiin sosiaalisessa
mediassa, erityisesti Youtube-palvelussa, jaettujen aineistojen perusteella. Muiden
käyttäjien kokemukset analysoitiin tekoälyavusteisesti ChatGPT-työkalun avulla.

Tutkimuksen perusteella pelillinen murtautumistestauksen harjoittelu on kiinnostava
koulutusmuoto, joka vaikuttaa oikein kohdennettuna positiivisesti oppimiseen sekä
tietoturvatietoisuuden lisääntymiseen. Harjoittelumuoto ei kuitenkaan työläytensä
puolesta sovi harjoitusmuotona laajamittaiseen käyttöön. Murtautumistestauksen har-
joittelu sopii osaksi koulutustarjontaa käytettäväksi rajatuissa tapauksissa vastaa-
maan kohdennettua koulutustarvetta. Koulutusmenetelmällä voidaan muuttaa asen-
teita sekä työskentelytapoja tukemaan paremmin tietoturvallisia käytänteitä. Jatkotut-
kimukseksi suositellaan kuitenkin tutkimusaineiston laajentamista useampaan otok-
seen, kattamaan laajemmin eri harjoittelualustoja ja kokonaisuuksia sekä kehittä-
mään rinnakkaisanalyysiä käyttäjän ja tekoälyavusteisen työkalun kanssa.

Avainsanat: Murtautumistestaus, Tietoturvatietoisuus, Koulutus

Tämän opinnäytetyön alkuperä on tarkastettu Turnitin Originality Check -ohjelmalla.

Abstract

Author: Joni Sirkiä
Title: Applicability of penetration testing training as a tool for increasing cyber security awareness
Number of Pages: 59 pages + 2 appendices
Date: 1 November 2024

Degree: Bachelor of Engineering
Degree Programme: Degree Programme in Information and Communication Technology
Professional Major: Information and Communication Technology
Supervisors: Janne Salonen, Director of school

With the growing integration of internet-connected information systems and digital resources in our daily lives, exposure to cybersecurity threats has significantly increased. Enhancing cybersecurity awareness is essential in mitigating these risks. However, traditional training methods have various challenges and limitations. This research examines a gamified penetration testing as a tool for increasing cyber security awareness. Aim of this study is to assess the effectiveness and applicability of this type of training method as a tool for raising cybersecurity awareness.

The research was conducted as a mixed-methods study, combining a literature review and qualitative reflection research methods. The literature review established the theoretical framework and explored the role of penetration testing in cybersecurity. The qualitative analysis included researcher's own experiences training with TryHackMe platform and an AI-assisted comparative study of peer user experiences. Peer insights were gathered from social media sources, particularly YouTube, and analyzed using the ChatGPT tool for AI-assisted comparative research.

Findings suggest that gamified training of penetration testing can positively impact learning and cybersecurity awareness when targeted correctly. However, due to the time-intensive nature of these exercises, the method may not be suitable for widespread usage. The method can be effective in addressing targeted educational needs for selected user groups by influencing attitudes and practices and promoting secure behaviors. Further research should expand the participant base and consider alternative training platforms and trainings as well. Also, the method for creating comparative insights with AI-assisted tools should be studied further to generate more comprehensive understanding on applicability of such method for qualitative research.

Keywords: Penetration Testing, Cybersecurity Awareness, Training

Sisällys

Lyhenteet

1	Johdanto	1
2	Menetelmät	5
2.1	Kirjallisuustutkimus murtautumistestauksesta ja tietoturvatietoisuudesta	5
2.2	Laadullinen tutkimus tietoturvatietoisuuden parantamisesta murtautumistestausta harjoittelemalla	6
3	Tulokset	9
3.1	Tietoturvatietoisuudesta tietoturvallisuuteen	9
3.2	Murtautumistestauksesta tietoturvatietoisuuteen	12
3.3	Murtautumistestauksen harjoittelualustan valinta	18
3.4	Murtautumistestauksen harjoittelu valitulla alustalla	22
3.5	Muiden käyttäjien kokemukset murtautumistestauksen harjoittelusta valitulla alustalla	29
4	Tulosten arviointi	36
4.1	Omien kokemusten arviointi	36
4.2	Muiden käyttäjien kokemukset	41
4.3	Tulosten tulkinta	46
5	Yhteenveto ja keskustelu	47
	Lähteet	50

Liitteet

Liite 1: Esimerkkisyöte (ChatGPT)

Liite 2: Esimerkkituloste (ChatGPT)

1 Johdanto

Internetiin kytketyt tietojärjestelmät ja tietoaaineistot ovat entistä kiinteämmin osa jokapäiväistä elämäämme niin yksityis- kuin työelämässämme. Nämä järjestelmät ja aineistot ovat alttiita verkkorikollisuudelle ja altistavat yksilöt ja yhteisöt merkittäville riskeille (Traficom, 2023a). Viimeaikainen kiihtyvä verkkorikollisuuden kasvu on korostanut tietoturvallisuuden tärkeyttä (Traficom 2022, DVV 2024).

Viimeaikainen tietoturva- ja tietoturvaympäristön kehitys ja Ukrainan tilanne ovat muuttaneet tilannetta tietoturvakentällä (Joensuu, 2023; Rautakoura, 2023; Huntley, 2023), mikä on näkynyt esimerkiksi valtiollisesti tuettujen toimijoiden aktiivisuudessa ja toiminnan kohdentumisessa. Viime aikoina on ukrainalaisiin hallintoelimiin sekä infrastruktuuriin kohdentuneiden toimien lisäksi lisääntyneet myös NATO-maihin kohdennetut verkkourkintahyökkäykset (*spear-phishing*). Samaan aikaan on itä-eurooppalaisissa (tieto)rikollisuusryhmissä sekä laajemmassa ekosysteemissä tapahtunut muutoksia poliittisen suuntautuneisuuden ja geopolitiikan mukaisesti, minkä on muuttanut ja tulee myös muuttamaan tietoturvakenttää lähiaikoina. Yleisesti kiristynyt kyberturvallisuustilanne sekä tiettyjen toimijoiden toiminnan kohdentuminen NATO-maihin vaikuttaa myös Suomessa toimiviin yrityksiin ja yhteisöihin (Huntley, 2023.; Joensuu, 2023). Kiristyneen kyberturvallisuustilanteen voidaan ajatella korostavan tietoturvan tärkeyttä niin yrityksissä kuin ihmisten yksityiselämässämme.

Tietoturvalla (myös tietoturvallisuus) tarkoitetaan tässä yhteydessä yleisesti järjestelmien teknologioita ja prosesseja, joilla pyritään suojaamaan tietoverkkoja ja aineistoja luvattomalta käsiksi pääsylvä sekä muulta haitan aiheuttamiselta, joita vihamieliset toimijat (verkkorikolliset, terroristit ja hakkerit) pyrkivät aiheuttamaan. Yleisesti ottaen tietoturvana voidaan puhua järjestelyistä, joilla varmistetaan tiedon luottamuksellisuus, eheys ja saatavuus (Sanastokeskus: TEPA-termipankki). Terminologista tietoturvan määritelmää on kuvattu laajemmin esimerkiksi kyberturvallisuuskeskuksen sivuilla (Traficom, 2023a).

Tiedon luottamuksellisuuden, eheyden tai saavutettavuuden pettäminen muodostaa riskin, jonka toteutumisen vaikutukset voivat olla hyvinkin merkittävät. Yrityksille tämä voi tarkoittaa miljoonien eurojen kustannusvaikutuksia (WEF 2024). Joissain tapauksissa vaikutuksena voi olla merkittävä yksilötason luottamuksen menetys (Mäki, 2022) tai tietojen pysyvä menettäminen (ICO n.d.)

Tietoturvan pettämisen vakavuutta kuvaavia tapahtumia on useita esimerkiksi vuonna 2021 kiristyshaittaohjelma sulki Yhdysvalloissa merkittävän polttoaineen jakelijan operaatiot useiksi päiviksi aiheuttaen laajaa kaaosta ja polttoainehintojen kohoamista sekä uhkan jakelun katkeamisesta useilla alueilla (Bing & Kelly, 2021). Tilanne raukesi yrityksen maksaessa useiden miljoonien dollareiden lunnaat. Toisessa tapauksessa tietovuodon kohteeksi joutunut teleoperaattori joutui maksamaan 350 miljoonaa dollarin korvaukset asiakkailleen (Washington Post, 2022). Vastaavasti vuonna 2017 paljon julkisuuttakin saaneen NotPetya tapahtuman vaikutukset, jossa merkittävä määrä yritysten dataa tuhoutui kyberhyökkäyksessä, olivat globaalisti arvioituna jopa 10 miljardia dollaria. Esimerkiksi Maerskille aiheutuneen vaikutuksen on arvioitu olleen noin 300 miljoonaa dollaria, TNT Expressille noin 400 miljoonaa dollaria ja Merckille noin 870 miljoonaa dollaria (Capano, D. E., 2023). Suomalaisena esimerkkinä voidaan nostaa esimerkiksi Vastaamon tapaus (RIKUteema, 2/2022), jossa tietomurron seurauksena merkittävä määrä yksityisen psykoterapiakeskuksen asiakkaiden potilas- ja henkilötietoja vuodettiin (Kortesoja, 2022).

Vastaava tietoturvariski kohdistuu myös erilaisiin yhteiskunnan toiminnan kannalta tärkeisiin tehtäviin. Esimerkiksi riski maatalouteen kohdistuvista iskuista on kohonnut erilaisten uusien teknologioiden yleistymisen myötä (Kulkarni ym. 2024; Hartley, 2022) tai jopa terveystalouden tuottaminen tai potilaiden henki voi olla uhattuna tietoturvan pettäessä (Tidy, 2022.)

Tietoturvan yhteiskunnallista vaikuttavuutta voidaan tarkastella esimerkiksi taloudellisten vaikutusten kautta. IBM:n tekemän selvityksen (IBM, 2022) mukaan tietomurron keskimääräinen kustannus yrityksille globaalisti oli vuonna 2022 13% enemmän kuin vuonna 2020, noin 4 miljoonaa euroa. Selvityksen mukaan

Pohjoismaissa keskimääräinen kustannus oli noin puolet globaalista keskiarvosta. Vastaavasti massiivisten tietomurtojen (yli miljoona tietuetta) kustannukset nousivat vuonna 2021 jopa 350 miljoonaan euroon. Tietomurtojen yleisimpänä syynä oli vuonna 2022 tunnusten varastaminen tai muuten vaarantuminen. Muita yleisiä hyökkäysvektoreita olivat kalastelu, pilvialusten virheellinen määrittely sekä kolmansien osapuolien ohjelmat. Tapahtuvien tietomurtojen kustannuksiin merkittävästi vaikuttavia tekijöitä (100 000–300 000 euroa tapausta kohden) olivat vuonna 2021 muun muassa tekoälyalustat, DevSecOps lähestyminen, tiedon salaustekniikoiden käyttö, henkilöstön koulutus sekä erilaiset eettisen hakkeroinnin menetelmät kuten murtautumistestaus sekä muut ”punaisen tiimin” testaukset. (IBM 2022)

Tietoturvallisuuden kokonaisuuteen kuuluu näiden vaikutusten (riskien) pienentäminen. Riskienhallintatoimenpiteenä tietoturvaa voidaankin tarkastella sellaisten tietoturvajärjestelyiden kautta, joiden tavoitteena on riskin toteutumisen todennäköisyyden pienentäminen tai vaikutusten pienentäminen erilaisin keinoin. Yhtenä tällaisena toimenpiteenä voidaan pitää yleisesti organisaation tietoturvatietoisuuden lisäämistä, jota voidaankin pitää linkittyneenä kasvavaan ymmärrykseen tietoturvallisuudesta (Zwilling ym. 2022). Toisena tärkeänä toimenpiteenä voidaan pitää tarkoituksenmukaisen turvallisuustason jatkuvaa seurantaa ja ylläpitoa esimerkiksi eettisen hakkeroinnin keinoin.

Eettisen hakkeroinnin tarkoituksena on selvittää, millaista haittaa pahantahtoinen toimija voisi aiheuttaa, jotta oma toiminta kyetään suojaamaan tarvittaessa (Palmer, 2001). Yksi eettisen hakkeroinnin keino järjestelmien turvallisuustason seurantaan ja tutkimiseen on murtautumistestaus (*penetration testing*), jolla pyritään tunnistamaan järjestelmästä heikkouksia mahdollisia korjaavia toimenpiteitä varten ennen kuin vihamielinen toimija pääsee näiden heikkouksien kautta aiheuttamaan haittaa (IBM 2022). Osana laajempaa tietoturvakokonaisuutta voidaan murtautumistestaus nähdä riskienhallintatoimenpiteenä, jonka tarkoituksenmukainen laajuus riippuu niin suojattavasta ympäristöstä itsestään kuin toimijan valitsemasta riskienhallintastrategiasta (Vegesna, 2023).

Toisena ja yhtenä tärkeimmistä tekijöistä tietoturvallisuuden näkökulmasta (Tsohou ym. 2008) voidaan nostaa esille tietoturvaluustietoisuuden rooli sekä sen lisäämisen kohentava vaikutus tietoturvaan yleisesti (Khando ym., 2021). Tietoturvaluustietoisuuden lisäämistä voidaan edesauttaa erilaisin menetelmin, kuten erilaisin tietoisuuskurssin, ohjaajan vetämin esitelmin tai harjoitustilaisuuksin, tai erilaisin verkkopohjaisiin menetelmin, kuten harjoituksiin, erilaisin viestein tai pelillisiin menetelmin (Alotaibi & Alfehaid, 2018). Pelillinen harjoittelu voi tietoturvaluustietoisuuden parantamisen lisäksi myös muuttaa yleisiä asenteita suotuisimmiksi muilla menetelmillä toteutettuja koulutuksia kohtaan (Ghazvini and Shukur 2018).

Tässä tutkimuksessa tarkastellaan murtautumistestausta osana tietoturvaluuden kokonaisuutta, turvallisuustason seurannan työkaluna, sekä sen harjoittelun soveltuvuutta tietoturvaluustietoisuuden ja yleisen turvallisuustason lisäämiseksi.

Murtautumistestausta sekä sen linkittymistä tietoturvaluuteen tarkastellaan sekä kirjallisuustutkimuksena että käyttäjälähtöisen tutkimuksen näkökulmasta. Käyttäjälähtöisessä tutkimuksessa käyttäjä tutustuu avoimesti verkossa olevien alustojen kautta murtautumistestauksen menetelmiin sekä kenttään yleisluontoisesti. Reflektioivan kokemukseen perustuvan laadullisen tutkimuksen avulla tarkastellaan, miten murtautumistestauksen harjoittelu soveltuu tietoturvaluustietoisuuden lisäämisen työkaluksi yleisellä tasolla.

Tutkimuksen tavoitteina on koota yleiskuva murtautumistestauksesta sekä arvioida murtautumistestausalustojen soveltuvuutta yleisesti tietoturvaluuden kehittämiseksi.

Tämän johdantokappaleen jälkeen kuvataan tutkimuksessa käytetyt tutkimusmenetelmät sekä luodaan työn teoreettinen viitekehys. Menetelmäkuvausten ja teoreettisen viitekehysten jälkeen kuvataan saadut tutkimustulokset sekä keskustellaan tutkimustulosten tarkoituksesta sekä soveltuvuudesta laajempaan

kontekstiin. Lopuksi esitetään yhteenveto ja suositukset tutkimustulosten hyödyntämiseen jatkossa muissa yhteyksissä.

2 Menetelmät

Tässä luvussa esitetään tutkimuksessa käytetyt tutkimusmenetelmät. Tutkimusmenetelmät koostuvat kirjallisuuskatsauksesta sekä laadullisesta tutkimuksesta. Kirjallisuuskatsauksessa tarkastellaan murtautumistestauksen roolia tietoturvatietoisuuden ja yleisen tietoturvallisuuden osana. Laadullisessa tutkimuksessa tarkastellaan refleктоivaan käyttäjäkokemukseen perustuen pelillisten murtautumistestausalustojen soveltuvuutta tietoturvaluustietoisuuden lisäämiseen organisaatiossa.

2.1 Kirjallisuustutkimus murtautumistestauksesta ja tietoturvatietoisuudesta

Työn ensimmäisen osan muodostaa kirjallisuustutkimuksena laadittu yleinen katsaus murtautumistestaukseen ja sen rooliin osana laajempaa tietoturvallisuuden kokonaisuutta. Laaditun kirjallisuuskatsauksen tarkoitus on luoda tutkimuksen teoreettinen viitekehys. Teoreettinen viitekehys muodostetaan esittämällä aiheeseen liittyvää tutkimuskirjallisuutta sekä määrittelemällä tutkimuksessa käytettävät käsitteet tutkimuskirjallisuuteen pohjautuen. Työssä esitetty kirjallisuuskatsaus on tyypiltään kuvaileva kirjallisuuskatsaus (Marjamaa & Sinisalo, 2022), jonka tarkoituksena on luoda yleiskuva tutkimuksen aihepiiristä. Kirjallisuuskatsaus on orientaatioltaan narratiivinen yleiskatsaus (Salminen, 2011).

Kirjallisuuskatsaus esittelee erään eettisen hakkeroinnin menetelmän, murtautumistestauksen, yleisesti sekä osana laajempaa tietoturvallisuuden kokonaisuutta. Katsaus käsittelee myös harjoittelun vaikutuksia ymmärryksen tietoturvasta kasvamiseen ja sitä, miten ymmärryksen kehittäminen edistää yleisesti tietoturvallisuutta organisaatiotasolla.

Yleiskuvan muodostamisen lisäksi kirjallisuuskatsauksen perusteella tarkennettiin toisen vaiheen tutkimusongelmaa ja tutkimuskysymyksiä sekä tutkimusasetelmaa tutkimuskirjallisuudesta esiin nousseiden havaintojen perusteella.

2.2 Laadullinen tutkimus tietoturvatietoisuuden parantamisesta murtautumistestausta harjoittelemalla

Laadullinen tutkimus koostuu kahdesta osasta: tutkijan kokemusperäisestä reflektioivasta tutkimuksesta sekä muiden käyttäjien kokemusten arviointitutkimuksesta.

2.2.1 Kokemusperäinen reflektioiva tutkimus

Tutkimuksen toinen osa muodostuu laadullisesta tutkimuksesta, jossa arvioidaan murtautumistestauksen harjoittelun soveltuvuutta tietoturvatietoisuuden lisäämiseen ja näin tietoturvallisuuden parantamiseen. Tutkimusmenetelmänä on käytetty kokemusperäistä reflektioivaa tutkimusta, jossa tutkija harjoittelee murtautumistestausta verkkopohjaisella harjoittelualustalla ja arvioi (reflektoi) kokemuksiaan. Näiden kokemusten perusteella arvioidaan, kuinka tällainen pelillistetty harjoittelu voi vaikuttaa tietoturvallisuuteen yleisesti.

Tutkijan omaan kokemukseen ja havaintoihin perustuva reflektioiva tutkimusprosessi on laajalti hyväksytty ja paljon käytetty laadullinen tutkimusmuoto. Tällaisessa tutkimuksessa tarkoituksena on tehdä näkyväksi tutkimustulokset, jotka juontavat juurensa tutkijan tekemiin valintoihin ja päätöksiin sekä kuvata avoimesti syyt, miksi tällaisiin tiettyjä valintoja ja johtopäätöksiä on tehty. Tavoitteena on samalla luoda selkeä kuvaus siitä, miten tutkijan omat kokemukset, arvot ja muu maailmankuva vaikuttavat tutkimukseen. Näin tutkimuksessa tuodaan avoimesti näkyväksi ja tulosten tulkinnan osalta muiden arvioitaviksi tutkijan henkilökohtaisten vinoumien (*bias*) mahdollinen vaikutus tutkimuksen tuloksiin sekä tehtyjen johtopäätösten hyödynnettävyyteen muissa yhteyksissä. (Orttilipp, 2008)

Tutkimusmenetelmässä on oleellista, että tutkija seuraa ja dokumentoi jatkuvasti tekemäänsä tutkimusta, ja tämän osalta heijastelee (reflektoi) mietteitään ja kokemuksiin, jotta nämä löydökset ovat käytettävissä tutkimuksen tuloksia analysoitaessa. (Ortilipp, 2008)

Tässä tutkimuksessa tutkija harjoittelee murtautumistestausta verkkoalustalla (TryHackMe.com), suorittamalla verkkoalustan tarjoaman opiskelupolun (Jr Penetration Tester) sekä reflektoi kokemuksiin tämän harjoittelun aikana. Tutkijan kokemusten perusteella puolestaan pyritään arvioimaan vastaavan menetelmän yleistettävyyttä keinoksi parantaa tietoturvasuorituksia yleisesti.

2.2.2 Koostetutkimus muiden käyttäjien kokemuksista

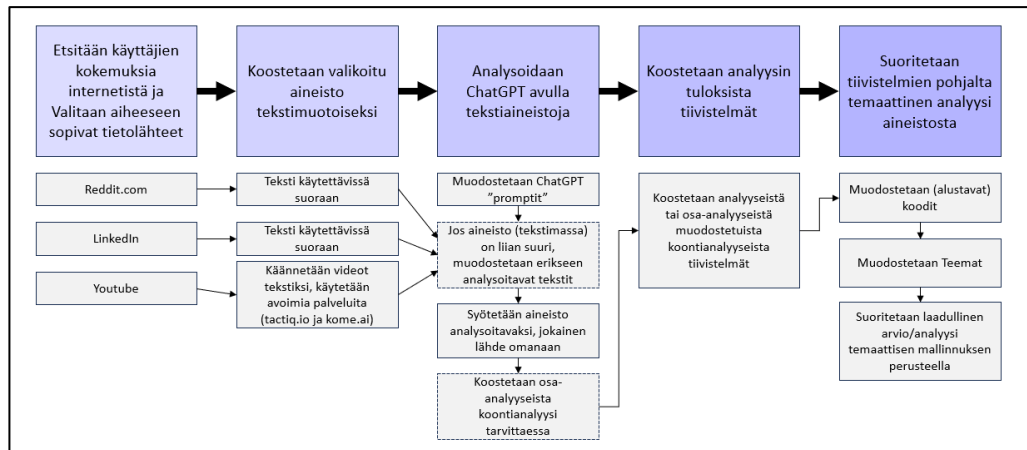
Muiden käyttäjien kokemuksia analysoiva koostetutkimus toteutetaan keräämällä muiden käyttäjien kokemuksia keskustelufoorumeilta sekä sosiaalisesta mediasta, sekä analysoimalla näitä tekoälyavusteisesti. Tekoälyavusteisella menetelmällä tarkoitetaan tässä työssä laajoihin kielimalleihin (LLM/NTP) perustuvia sovellutuksia (tässä työssä ChatGPT). Nämä menetelmät ovat yleistyneet viime aikoina merkittävästi, mikä tarjoaa merkittäviä mahdollisuuksia laadullisen tutkimuksen tehostamiseen. (Zhang ym. 2023; Turobov ym, 2024). Tekoälyavusteista tutkimusta käytetään tässä työssä refleктоivan tutkimuksen luotettavuuden analysointiin sekä yleisesti valitun menetelmän käytettävyyden arviointiin.

Tässä tutkimuksessa käytetty työkalu "ChatGPT" on OpenAI:n tuote, joka perustuu suuriin kielimalleihin (LLM). ChatGPT:n taustalla on koulutetut generatiiviset tilastolliset mallit, joiden avulla ohjelma kuuntelee sekä vastaa sujuvasta työkalun käyttäjälle. Ohjelman toiminta perustuu sen itse rakentamaan neuroverkkoon, ja vaikka ohjelman toiminta vaikuttaa vastaavan ihmismielen toimintaa se perustuu tilastollisiin malleihin ei syvempään ymmärrykseen tai tietoisuuteen. (Turun Yliopisto, 2024.; Haque & Li, 2024).

Vaikka näihin menetelmiin liittyy monia epävarmuuksia erityisesti tieteellisen tutkimuksen luotettavuuden ja eettisyyden näkökulmasta, tarjoaa näiden menetelmien käyttö merkittäviä hyötyjä tutkimusprosessille, kun menetelmiä käytetään varsinaisen tutkimuksen rinnalla sitä avustavassa roolissa. (Turobov ym., 2024).

Tässä työssä käytetty tekoälyavusteinen analyysiprosessi on kuvattu alla kuvassa 1. Ensimmäisessä vaiheessa etsitään muiden käyttäjien kokemuksia internetistä ja valitaan tarkoitukseen sopivimmat tietolähteet. Tähän tutkimukseen valittiin tietolähteiksi keskustelufoorumi Reddit.com, työelämään keskittyvä verkoyhteisöpalvelu LinkedIn sekä sosiaalisen median alusta Youtube. Näistä tietolähteistä koottu aineisto koottiin tekstimuotoiseksi lähtöaineistoksi. Reddit-palvelun sekä LinkedIn palvelun aineistot olivat käytettävissä sellaisenaan. Youtube-palvelun videosisällöt käännettiin tekstimuotoisiksi avoimia palveluita hyödyntäen (tactiq.io sekä kome.ai). Näin muodostettiin tekoäly-apurille sopiva tekstimuotoinen lähtöaineisto.

Ennen syöttämistä ChatGPT:lle, valmisteltiin myös syötteet, joilla ohjattiin tekoälyapurin työtä. Syötteet valmistettiin mukauttamalla Turobov ym. (2024) käyttämää analyysirutiiniä tähän tutkimukseen soveltuvaksi. Käytetyt syötteet on esitetty liitteessä 1. ChatGPT:lle syötettiin analysoitavaksi kerätty tekstimuotoinen aineisto näiden syötteiden avulla. ChatGPT-analyysit on tehty ilmaisella lisensillä syyskuun 2024 aikana, jolloin käytössä on ollut GPT-4o mini sekä GPT-3.5-mallit. Tekstiaineistot, joiden koko oli syötteineen yli 4000 sanaa, on jaettu erilliseksi osa-aineistoiksi (alle 4000 per aineisto), jotta nämä saatiin analysoitua valitulla työkalulla. Osa-aineisto-analyysit koostettiin vastaavasti yhteen koonti-analyysiksi syöttämällä nämä osa-analyysit erikseen uutena lähtöaineistona ChatGPT:n analysoitavaksi. Esimerkki ChatGPT:n muodostamasta analyysistä on esitetty liitteessä 2. Analyysissa koottiin nämä tekoälyavusteiset analyysit tiivistelmiksi, jotka on esitetty tämän työn Tulokset-kappaleessa. Lopuksi muodostetuille tiivistelmille tehtiin temaattinen analyysi, jonka pohjalta arvioitiin työn tutkimuskysymyksiä.



Kuva 1. Tekoälyavusteisen analyysin prosessi

3 Tulokset

3.1 Tietoturvatietoisuudesta tietoturvallisuuteen

Tässä kappaleessa tutustutaan kirjallisuuskatsauksen keinoin tietoturvallisuuden rooliin ja tärkeyteen osana laajempaa tietoturvallisuutta.

Yksi oleellisimmista tietoturvallisuuden osa-alueista on tietoturvallisuustietoisuus sekä sen lisääminen yleisesti (Khando ym., 2021). Toisaalta termiä tietoturvatietoisuus käytetään kirjallisuudessa vaihtelevasti tarkoittamaan eri laajuisia kokonaisuuksia, joihin voi sisältyä harjoittelua tai koulutusta, tai jotka voivat jopa käsittää prosessina tietoisuuden kehittämisen (Tsohou, 2008). Tässä työssä tietoturvallisuustietoisuudella tarkoitetaan käyttäjien ymmärrystasoa tietoturvaan liittyviin riskeihin sekä tietoturvallisuuden parhaisiin käytänteisiin liittyen (Abawajy, 2012). Tietoturvatietoisuuden lisäämistä käsitellään puolestaan Tsohou ym. (2008) mukaisesti prosessina, joka pyrkii muuttamaan yksilöiden näkemyksiä, arvoja, asenteita, käyttäytymistä, normeja, työskentelytapoja sekä organisaation kulttuuria ja rakenteita tukemaan paremmin tietoturvallisia käytänteitä.

Tietoturvatietoisuus on nostettu yhdeksi tärkeimmistä tekijöistä tietoturvallisuuden näkökulmasta. Valitettavasti organisaatiot eivät kuitenkaan ole yleensä toteuttaneet riittäviä toimenpiteitä tietoturvatietoisuuden kehittämiseksi. (Tsohou ym. 2008). Merkittävä määrä tietoturvapoikkeamista johtuukin inhimillisen tekijän (*human element*) hyväksikäytöstä. Näin ollen tarkoituksenmukaisen turvallisuustason saavuttaminen ja ylläpitäminen ei ole mahdollista ilman, että inhimilliseen toimintaan panostetaan tietoisuuden lisäämisen ja koulutuksen kautta (Bresz, 2004). Tietoturvatietoisuuden lisäämistä voidaankin pitää yhtenä kriittisistä tekijöistä tiedon suojaamisessa (Khando ym., 2021).

Useat standardit, kuten NCSC, NIST, IEC-62443 ja ISO-27001 nostavat esiin kouluttamisen ja tietoisuuden kehittämisen työntekijöiden parissa yhtenä oleellisimmista vastatoimista tietoturvariskejä vastaan (Hart ym., 2020). Perustavanlaatuisena periaatteena voidaankin pitää sitä, että organisaatioiden tulee varmistaa kaikkien työntekijöiden kouluttaminen tietoturvahyökkäysten muodostamien riskien suuruudesta sekä tekemään turvallisempia päätöksiä ja toimia näiden riskien lieventämiseksi (Hart ym., 2020). Näin ollen yhtenä merkittävämpanä esteenä tietoturvallisuuden lisäämiselle onkin kiinnostavien ja sopivien koulutusmateriaalien puuttuminen (Bada ym., 2019).

Tietoturvatietoisuuden lisäämiseksi on useita menetelmiä. Yleinen käytäntö tietoturvallisuustietoisuuden lisäämiseksi on luokkahuone tai tietokoneen välityksellä tehtävä tietoisuuskoulutus. Vaikka tällainen menetelmä onkin hyvä teoreettinen lähtöpiste, se ei ole riittävä menetelmä kompleksisten tietoturvakonseptien hallitsemiseksi (Hart ym., 2020).

Kompleksisuus haasteen lisäksi kulloiseenkin tilanteeseen sopivan menetelmän valinnassa on huomioitava lisäksi menetelmän soveltuvuus erilaisille henkilöille, sillä henkilökohtaiset näkemykset, uskomukset ja vinoumat vaikuttavat merkittävästi yksilön toimintaan (Tsohou ym., 2015). Monesti haasteena on motivaationaalisten tekijöiden puute osana koulutuksia (Alshaikh ym., 2018). Yleisesti voidaankin ajatella, että eri menetelmien yhdistäminen on suositeltava ratkaisu (Abawajy, 2012).

Tässä työssä keskitytään tarkastelemaan erityisesti viime aikoina yleistynyttä (Swann ym., 2021) menetelmää tietoturvaluustietoisuuden lisäämiseksi: pelillistämistä, joka tietoturvaluustietoisuuden parantamisen lisäksi voi muuttaa yleisiä asenteita suotuisimmiksi muilla menetelmillä toteutettuja koulutuksia kohtaan (Ghazvini and Shukur 2018). Esimerkiksi Khan ym. (2011) havaitsi, että vuorovaikutteiset koulutusvaihtoehdot kuten videopelit motivoivat ja tempaavat mukaansa huomattavasti paremmin kuin niitä perinteisemmät menetelmät. Näin ollen tällaiset menetelmät soveltuvat hyvin aseteiden muuttamiseen ja ovat hyvin räätälöitävissä tilanteen mukaan (Flores and Ekstedt, 2016; Khando ym., 2021), vaikka soveltuvatkin laajempaan tiedonsiirtoon tai opetukseen vain rajallisesti.

Pelillistämisen on havaittu johtavan lisääntyneeseen motivoituneisuuteen sekä tietoturvaluustietoisuusmenetelmien käyttöön (Khando ym., 2021). Pelillisten harjoitusten tekeminen johtaa tietoturvakonseption nopeampaan oppimiseen ja laajempaan ymmärrykseen (Gjersten ym., 2017). Pelillistäminen lisää tietoturvaluustietoisuutta sekä muuttaa asenteita suotuisemmiksi tietoturvatietoisuus-koulutusta kohtaan, sillä pelillistäminen koetaan yleisesti mukavaksi sekä helposti lähestyttäväksi tavaksi käsitellä asiaa (Ghazvini and Shukur 2018).

Vaikka ryhmäkeskustelut ja esitykset ovat tehokkaampia menetelmiä laajojen kokonaisuuksien opettamiseen sekä lyhyiden tietoiskujen antamiseen. Pelillisten menetelmien etuna on erityisesti asenteisiin voimakkaammin vaikuttaminen sekä syvällisemmän ymmärryksen ja osaamisen tuottaminen. Erityisesti tällaisten menetelmien etuna on niiden räätälöitävyys henkilökohtaisiin tarpeisiin sekä vapaus erilaisten realististen skenaarioiden luomiseen. (Karagiannis ym. 2020; Khan ym. 2011). Voidaankin esimerkinomaisesti väittää, että opiskelijat muistavat noin 10 prosenttia lukemastaan, 20 prosenttia kuulemastaan ja puolet näkemästään, mutta jopa 90 prosenttia itse tekemistään asioista, vaikka nämä asiat olisikin tehty simuloitulla alustalla (Jelo & Helebrandt, 2022).

Yhtenä esimerkkinä tietoturvakentän pelillisistä menetelmistä voidaan pitää CTF- harjoituksia (*Capture The Flag*), joita tässä työssä tarkastellaan tarkemmin. CTF-harjoitus on haastemuotoinen peli, jossa osallistujia haastetaan erilaisten tietoturvan osa-alueiden tiimoilta. Erityisesti näiden haastetehtävien voidaan ajatella kehittävän teknistä osaamista tietoverkkojen turvallisuuteen liittyen, mutta se kuinka hyvin ne vastaavat inhimillisten tekijöiden haasteisiin kuten sosiaaliseen manipulointiin (*social engineering*) tai yleiseen tietoturvatietoisuuteen ei aina ole selvä. (Švábenský, ym., 2021).

Erilaisia CTF-alustoja ja menetelmiä lukuisia on lukuisia; näistä ehkä merkittävimpiä on kuvattu alle (Kuva 2) mukailten Ortiz-Garces (2023) esittämää koostetta.

	FBCTF	CTFd	HTB	PicoCTF	TryHackMe
Toiminnallisuus					
Visuaalisuus ja kilpailu	Haastekartta ja tulostaulukko	Haasteet, kategoriat, pisteet	Haasteet, kategoriat, pisteet	Haasteet, kategoriat, pisteet	Haasteet, kategoriat, pisteet
Dokumentaatio	Gitpage	Gitpage	Alustalla		
Käyttäjien luokittelu	Ei	Ei	Kyllä	Ei	Kyllä
Opetussisältö	Ei	Ei	Kyllä	Ei	Kyllä
Mainokset	Kyllä	Kyllä	Kyllä	Kyllä	Ei
Kategoriat					
Stegografia	Kyllä	Kyllä	Kyllä		
Kryptografia	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
OSINT	Kyllä	Kyllä			
Tietoverkon tietoturva	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
Perusteet	Kyllä	Kyllä			Kyllä
Käänteismallinnus	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
Ohjelmointi	Kyllä	Kyllä			Kyllä
Puhelimen tietoturva	Kyllä	Kyllä	Kyllä		
Forensiikka, analyysi	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä

Kuva 2. CTF-alustojen vertailu, Ortiz-Garces (2023) mukaan.

Muista kuin CTF pelillisistä menetelmistä mainittakoon *CyberCIEGE*, *Cyberprotect Hacknet* tai *NITE team4*, tai lautapelit kuten *Control-Alt-Hack* tai *OWASP Cornucopia*. (Karagiannis ym. 2020; Khan ym. 2011). Näihin vaihtoehtoisiin menetelmiin ei tässä työssä perehdytä tarkemmin.

3.2 Murtautumistestauksesta tietoturvatietoisuuteen

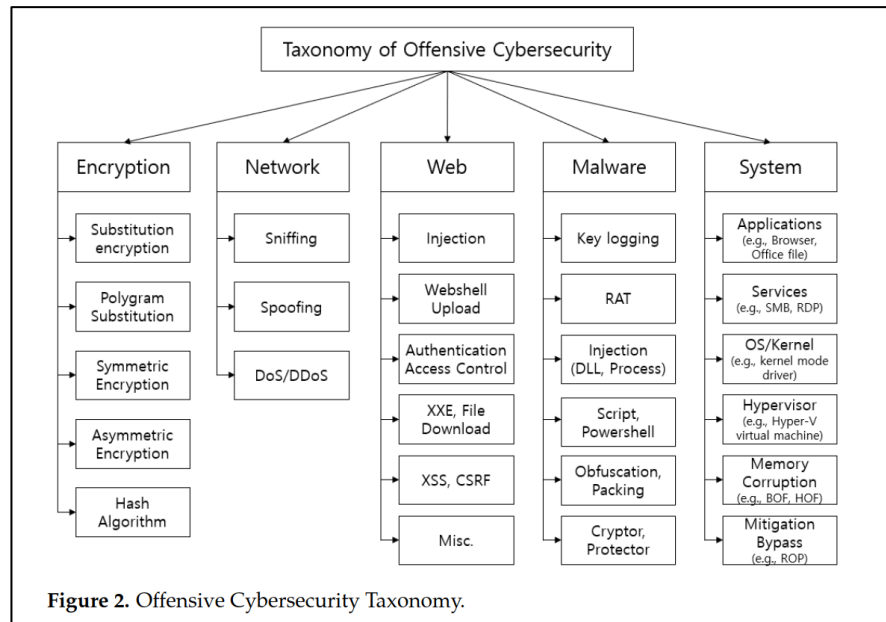
Tässä kappaleessa tutustutaan kirjallisuuskatsauksen kautta tarkemmin murtautumistestaukseen. Ensimmäisessä kappaleessa perehdytään murtautumistestauksen rooliin osana laajempaa tietoturvan kokonaisuutta. Toisessa kappaleessa tutustutaan puolestaan tarkemmin murtautumistestaukseen prosessina.

3.2.1 Murtautumistestaus osana kokonaispuolustusta

Hyökkäävä tietoturva, kuten murtautumistestaus, on oleellinen osa kokonaispuolustusta (DeValk ym., 2022). Murtautumistestaus mahdollistaa tietoturvaaukkojen löytämisen tietoverkoista tai ohjelmistoista mahdollistaen näiden korjaamisen tai niiden muodostamien riskien lieventämisen.

Tutkimuskirjallisuuden näkökulmasta hyökkäävän tietoturvan (myös eettinen hakkerointi) voidaan katsoa saaneen alkunsa 1990-luvun alkupuolella, jonka jälkeen se on kehittynyt ensin yksittäisten (eettisten) hakkereiden toiminnasta 1990- ja 2000-lukujen vaiheessa alkaneeseen järjestyneeseen, tietoturvayritysten harjoittamaan toimintaan (Paavola, 2014). Hyökkäävä tietoturva on sittemmin kehittynyt laajempaan tietoturvaasiantuntijoiden ja tutkijoiden osaamisen hyödyntämiseen monilla eri yhteiskunnan tasoilla ja rakenteilla. (Kim ym., 2021). Nykyään hyökkäävään tietoturvaan liittyy erityisasiantuntijoiden työn lisäksi myös enemmissä määrin erilaiset koneoppimismalleja hyödyntävät tekoälysovellukset (Aiyanyo ym., 2020).

Hyökkäävä tietoturva on monipuolinen kenttä, johon kuuluu mm. erilaisia salaukseen, tietoverkkojen yli tapahtuvaan vaikuttamiseen, selaimen kautta toimintaan, haittaohjelmiin sekä erilaisiin järjestelmiin luokiteltavia kokonaisuuksia. Alla on esitetty hyökkäävän tietoturvan kenttää taksonomian kautta, mukaillen Kim ym. (2021) esitystä. Yksittäisiä elementtejä ei tässä työssä esitetä sen tarkemmin.



Kuva 3. Hyökkäävän tietoturvan taksonomia Kim ym. (2021) mukaan.

Hyökkäävää tietoturvaa voidaan pitää ratkaisevan tärkeänä työkaluna järjestelmän heikkojen kohtien löytämiseksi tietoverkosta tai ohjelmistosta mahdollistaen näiden paikkaamisen sekä vaikutusten rajaamisen sekä lieventämisen (DeValk ym., 2022).

Murtautumistestauksesta osana hyökkäävää tietoturvaa on puolestaan ruvettu puhumaan 2000-luvun taitteessa (Paavola, 2014). Murtautumistestaus on hyökkäävän tietoturvan ja (eettisen) hakkeroinnin osa-alue, jossa murtautumistestaaaja (tai hakkeri) pyrkii testaamaan organisaation turvallisuutta erilaisin menetelmin. Murtautumistestauksella pyritään löytämään heikkouksia organisaation turvallisuudesta ja selvittämään voisiko ulkopuolinen toimija käyttää näitä heikkouksia hyväkseen sadakseen luvattoman pääsyn järjestelmään tai tietoon (Balloch, 2017).

Murtautumistestaukseen kuuluu oleellisena osana lupa tehdä testausta (eettisyys), jota vihamielisellä toimijalla ei vastaavasti olisi (Paavola, 2014). Murtautumistestaaajasta voidaankin käyttää nimitystä valkohattuhakkeri kuvaamaan toiminnan luvallisuutta. Vastaavasti luvattomasti toimivasta toimijasta voidaan käyttää termiä mustahattuhakkeri. Toiminnan eettisyyden näkökulmasta on

selvä, että valkohattuhakkeri toimii eettisen hakkeroinnin periaatteiden mukaan, kun taas mustahattuhakkeri ei näin toimi (toimii laittomasti). (Paavola, 2013). Toisaalta koska asiat eivät aina ole mustavalkoisia, jää näiden toimintamallien väliin kolmas luokka, harmaahattuhakkeri. Harmaahattuhakkeri ei lähtökohtaisesti hae toiminnallaan henkilökohtaista etua eikä vahingon tuottamista, mutta voi esimerkiksi kokea, että lakien mukaan toimiminen rajoittaa käytettäviä menetelmiä liikaa eikä näin mahdollista esimerkiksi riittävän tehokasta positiivista muutosta. Näissä tapauksissa ei aina ole selvää (on harmaata), onko toiminta eettistä vai ei. (Harper ym. 2022).

Eettisyyttä ei tässä työssä määritellä taikka tutkita sen tarkemmin. Yleisesti voidaan kuitenkin todeta, että ei ole aina selvää mikä on eettistä (oikein). On lisäksi huomattava, että laillisuus ei (välttämättä) tarkoita samaa kuin eettisyys. Toisin sanoen, aina ei lakien ja asetusten mukaan toimiminen ole eettistä, eikä vastaavasti lakien ja asetusten vastainen toiminta välttämättä ole epäeettistä. Kirjoittaja kuitenkin suosittelee vahvasti kaikkia noudattamaan niin murtautumistestauksessa kuin muussakin elämässä kaikkia lakeja ja asetuksia ja jättämään tarkemman kokeellisen etiikan tutkimuksen muille, esimerkiksi filosofeille.

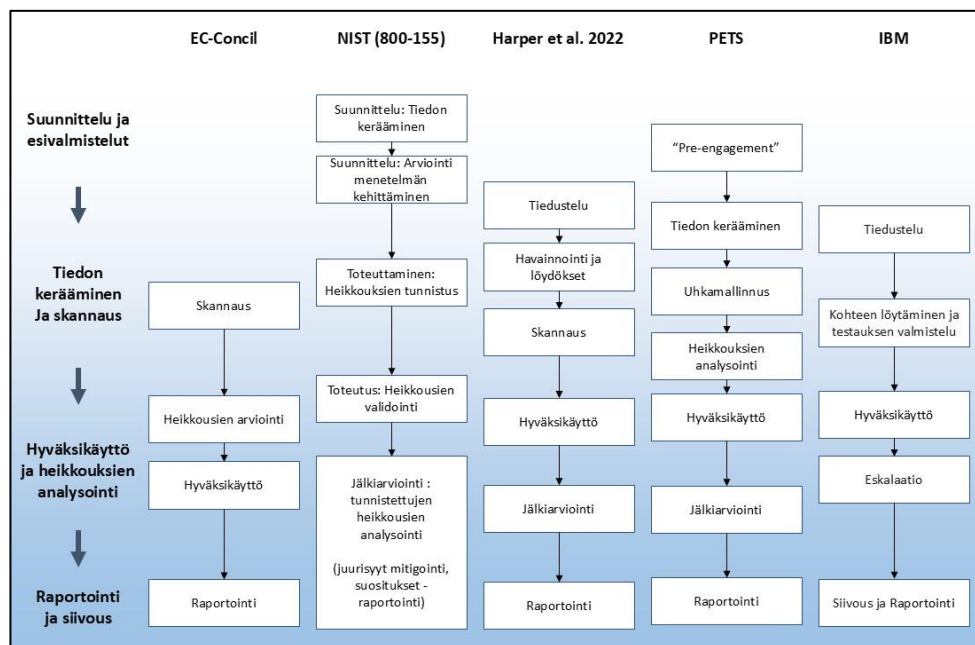
Murtautumistestausasetelmat voidaan luokitella käytettävissä olevan ennakkotiedon perusteella. Tilanteesta, jossa testaajalla on paljon ennakkotietoa käytettävissään, käytetään nimitystä *White box* -testaus. Vastaavasti *Black box* -testauksessa testaaja rinnastuu ulkopuoliseen toimijaan, jolla ei ole ennakkotietoa kohteesta. Näiden testausjärjestelyiden välimaastoon sijoittuu niin kutsuttu *Gray box* -testaus, jossa ennakkotietoa on jonkin verran käytettävissä. (Paavola, 2024). Tarkoituksenmukainen murtautumistestaukseen käytettävän ennakkotiedon määrä riippuu testauskohteesta ja testauksen luonteesta tapausittain.

Murtautumistestausta voidaan suorittaa keskittyen joko tietoverkkoihin, soveluksiin, fyysiseen ympäristöön, yksittäisiin laitteisiin tai pilviympäristöön. Monesti toteutettava eettisen hakkeroinnin kokonaisuus sisältää useita näistä vaihtoehdoista. (Harper ym. 2022).

Tässä työssä keskitytään ensisijaisesti tarkastelemaan tietoverkkojen välityksellä tapahtuvaa murtautumistestausta.

3.2.2 Murtautumistestausta prosessina

Murtautumistestausta voidaan ajatella prosessina tai projektina, johon kuuluu tietyt vaiheet. Erilaisia kuvauksia murtautumistestausta prosessista on useita, jotka kuitenkin mukailevat samaa teemaa. Yleisesti voidaan kuitenkin murtautumistestauksen vaiheet luokitella alkuvalmisteluihin, tiedon keräämiseen ja tunnisteluun, järjestelmän hyväksikäyttöön ja heikkouksien arviointiin sekä raportointiin ja siivoukseen. Erilaisia prosessikuvauksia on koottu alle (Kuva 4).



Kuva 4. Murtautumistestausta prosessina, yhdistetty eri lähteiden pohjalta (EC-Council, 2022; NIST 800-155; Harper ym., 2022; PTES, 2014; IBM, 2023)

Murtautumistestausta prosessin kuvaukset ovat tarkastelluissa lähteissä suhteellisen samankaltaiset, joskin eri lähteiden mukaisissa kuvauksissa on jonkin verran eroa erityisesti siinä millä tasolla eri vaiheiden sisältöä kuvataan. Esimerkiksi PTES (2014) kuvaa prosessin eri vaiheet suhteellisen tarkalla erotuksella erotellen tiedon keräämisen, uhkamallinnuksen ja heikkouksien analysoinnin

omiksi osioikseen, kun taas vastaava vaihe NIST 800-155-standardissa (NIST 800-155) on kuvattu yksinkertaisesti heikkouksien tunnistuksena. Lisäksi eri prosessikuvaukset eroavat siinä, onko tai millä tavalla on niissä kuvattuna jälkien siivoamista ja raportointia. Tai vastaavasti siinä, mistä murtautumistestausprosessin nähdään alkavan: onko esimerkiksi suunnittelu ja esivalmisteluvaihe osa itse testausprosessia. Prosessikuvauksiin kuvattujen vaiheiden eroista huolimatta on eri lähteiden kuvauksissa kuitenkin lähtökohtaisesti samansisältöiset kokonaisuudet.

Yleistettynä murtautumistestausprosessia voidaan kuvata seuraavasti. Ensin toteutetaan esivalmisteluvaihe, jossa määritetään toteutettavan testauksen laajuus (rajaaminen) ja sovitaan, millä keinoin testaus toteutetaan (mitä keinoja voidaan käyttää). Vaiheessa sovitaan myös mahdollisesti käytettävissä olevasta lisätiedosta järjestelmiin liittyen (White/Gray/Black Box). Vaiheeseen kuuluu yleisesti Työnkuvaus (Statement of Work eli SOW) sekä testauksen säännöt (Rules of Engagement eli ROW). Tätä vaihetta ei kaikissa prosessikuvauksissa ole sisällytetty itse testausprosessin kuvaukseen.

Toisena vaiheena tiedustellaan järjestelmää. Vaiheessa kerätään tietoa järjestelmästä erilaisin keinoin, kuten skannaamalla järjestelmää tietoverkkojen kautta. Tiedustelutieto kerätään yhteen ja analysoidaan sekä arvioidaan mahdollisia jatkotoimenpiteitä. Tiedusteluvaiheessa yhdistetään usein myös muilla keinoin saatuja tietoja; esimerkiksi julkisista lähteistä, kohteen työntekijöitä jututtamalla tai esimerkiksi aiemmin vuotaneita salasanalistoja hyödyntämällä. Vaiheen tavoitteena on kerätä riittävästi tietoa tutkittavasta järjestelmästä, jotta voidaan tunnistaa keinoja, joilla olisi mahdollista hyväksikäyttää järjestelmää tai sen ominaisuuksia asetettujen testaustavoitteiden mukaisesti.

Kolmantena vaiheena on kerätyn tiedon sekä tunnistettujen mahdollisten heikkouksien hyväksikäyttäminen osana suoritettavaa murtautumistestiä. Vaiheessa suoritetaan tiedustelun pohjalta tunnistettuja toimenpiteitä, joiden avulla pyritään saamaan ensin pääsy järjestelmään ja eskaloimaan oikeudet järjestelmässä riittävälle tasolle tavoitteiden (esim. tiedon hakeminen tai vahingon tekeminen)

saavuttamiseksi. Luonteeltaan kolmas vaihe on iteratiivinen prosessi, jossa pyritään kehittämään tunnistettujen heikkouksien pohjalta riittävän vaikutuksellinen kokonaisuus esimerkiksi linkittämällä tunnistettuja heikkouksia toisiinsa. Kolmas vaihe voi olla aikavaikutukseltaan hyvinkin pitkäkestoinen, jolloin korostuu tärkeys pääsyn ylläpitämiseen tai mahdollistamiseen uudelleen myöhemmässä vaiheessa. Lisäksi tässä vaiheessa korostuu vastatoimijan (puolustautuja) toimet, sillä mikäli testaajan toiminta havaitaan tulee testaajan kyetä toimimaan myös muuttuvassa tilanteessa, jossa vastatoimija pyrkii puolustautumaan (tai jopa hyökkäämään) testaajaa vastaan.

Murtautumistestauksen lopuksi peitetään jäljet, puhdistetaan järjestelmä ja raportoidaan testauksen löydökset, tulokset ja mahdolliset kehitysehdotukset testauksen pohjalta. Yleisesti voidaan ajatella, että raportoinnin tulisi sisältää tiivistelmä löydöksistä niin, että myös teknisesti vähemmän valveutunut lukija ymmärtää löydösten vaikutukset organisaatiolle, joskin jokainen testausasetelma on omanlaisensa ja näin ollen myös raportointi mukautetaan tilanteeseen.

3.3 Murtautumistestauksen harjoittelualustan valinta

Tässä kappaleessa tarkastellaan tutkimuksen harjoittelualustan valintaa kuvaamalla valinnan pohjaksi tehdyt arvioinnit ja vertailut. Ensimmäisessä aliluvussa esitetään muiden käyttäjien kokemusten analysointi. Toisessa aliluvussa puolestaan esitetään tutkijan tekemä itsearviointi.

3.3.1 Muiden kokemukset CTF alustan soveltuvuudesta ja eri alustoista

Yleisesti CTF-alustan soveltuvuutta tietoturvatietoisuuden parantamiseen arviointiin analysoimalla käyttäjän (Collins, G. 2023) kokemusten perusteella. Arviointi tehtiin noudattaen kappaleessa 2.2.2 esitettyä tekoälyavusteista tutkimusmenetelmää. Alle on koostettu tutkimusprosessin mukainen kooste puhujan näkemyksistä.

CTF-alustan soveltuvuuden arviossa nousi esille se, että puhuja korostaa erityisesti käytännön harjoittelun tärkeyttä, sillä tämä mahdollistaa puhujan mukaan erilaisten työkalujen ja skriptien testaamisen todellista elävää ympäristöä vastaavissa tilanteissa. Puhuja piti itse tästä ominaisuudesta paljon ja koki sen itselleen hyvin sopivaksi. Lisäksi puhuja mainitsee, että jatkuvasti haastavammaksi kehittyvä harjoittelu tuki oppimista sekä mahdollisti jatkuvan kehittymisen laaja-alaisen hyökkäysten kentässä. Harjoittelun ohessa opittuja lukuisia työkaluja ja tekniikoita pidettiin erityisen hyvinä, jopa kriittisinä, todellistietoturva haasteiden ratkomisen kannalta.

Toisaalta kriittisenä näkemyksenä CTF-alustan soveltuvuuteen arvioija nostaa esille harjoittelumuodon rajallisuuden yleisen ongelman ratkomisessa. Vaikka harjoittelu nähtiinkin kattavana, niin esimerkiksi erilaisten hyökkäysvektorien osalta harjoitusten rakenne koettiin joissain tapauksissa turhan suoraviivaisiksi, eikä niiden nähty tarjoavan riittävästi itsenäistä ongelmanratkaisua. Arvioija ehdottaakin, että alusta voisi tarjota laajemmin ja monipuolisemmin erilaisten vaihtoehtoisten ratkaisujen läpikäymistä oppimiskokemuksen parantamiseksi.

CTF-alustan sopivuuden arvioinnissa harjoittelumuodon vahvuudeksi koettiin henkilökohtaisen opiskelutahdin mahdollisuus sekä yleinen joustavuus. Lisäksi alusta koettiin yleisesti hyväksi ja soveltuvaksi opiskeluun. Erityisesti arvioija koki, että alusta ja harjoittelumuoto on hyvin tehokas niille, joille aihepiiri on entuudestaan vieras. Tietoturvatietoisuuden edistämisen näkökulmasta onkin tulkittavissa, että erityisesti kokemattomammille harjoittelijoille alusta tarjoaa paljon, ja että erityisesti todellisen maailman tilanteiden simulointi auttaa kehittymään.

Eri CTF-alustoja (tässä TryHackMe ja HackTheBox) vertailtiin käyttäjän kokemusten perusteella (InfoSec, P. 2023) vastaavalla, kappaleessa 2.2.2 esitetyllä menetelmällä. Arvioija pitää TryHackMe-alustaa hyvin soveltuvana tietoturvatietoisuuden sekä yleisten penetraatitestausten taitojen kehittämiseen erityisesti niille, jotka eivät entuudestaan tunne menetelmiä syvällisemmin. Vastaavasti HackTheBox nähdään soveltuvampana kehittyneemmille käyttäjille. Puhuja

suositteleekin aloittamaan ensin TryHackMe alustalle ennen HackTheBoxiin siirtymistä.

Näiden arvioiden perusteella CTF-alustalla harjoittelu voi olla tietoturvatietoisuutta parantava opiskelumuoto, joka soveltuu tässä tarkoituksessa erityisesti vähemmän murtautumistestausta tunteville käyttäjille. Vastaavasti TryHackMe alustaa voidaan pitää näille käyttäjille HackTheBox alustaa soveltuvampana harjoittelualustana.

3.3.2 Alustan ja oppimiskokonaisuuden arviointi ja valinta

Muiden käyttäjien kokemusten lisäksi arvioitiin alustaa sekä oppimispolkua sen perusteella, millainen vaikutelma näistä sekä muiden käyttäjien kokemuksista muodostui tutkijalle. On selvää, että erilaisia simuloituja murtautumistestauksen harjoitteluun sopivia alustoja on useita. Lisäksi vaikuttaa siltä, että alustat HackTheBox ja TryHackMe ovat näistä suosituimpia. TryHackMe koetaan yleisesti vähemmän aiheeseen perehtyneille sopivammaksi, joten sitä pidettiin tähän työhön soveltuvampana alustana.

TryHackMe vaikuttaa tarjoavan erilaisia pelillisiä oppitunteja, oppimispolkua sekä erillisiä yksittäisiä harjoituksia ja haasteita hyvinkin laajasti. Murtautumistestausta käsitteleviä oppimispolkua ovat erityisesti ”*Jr Penetration Tester*” -polku sekä ”*Offensive Pentesting*”-polku. ”*Jr Penetration Tester*”-polku luokitellaan helpommaksi kuin, ”*Offensive Pentesting*”-polku, joten sitä pidettiin tähän työhön paremmin soveltuvana vaihtoehtona.

Muiden käyttäjien kokemuksia, ja arvosteluja kyseisestä ”*Jr Penetration Tester*” oppimispolusta arvioitiin erilaisten keskustelufoorumien ja sosiaalisen median sisältöjen avulla (Reddit-keskustelu, 2022; Espinosa, 2023; Hon, 2023).

Näihin kokemuksiin perustuen, voidaan oppimispolkua pitää yleisesti keskivaikeana. Vaikka osa käyttäjistä onkin sitä mieltä, että polku sopii hyvin aloittelijoille, on osalla käyttäjistä ollut merkittäviä haasteita joidenkin osioiden kanssa.

Eriyisesti *Network Security* sekä *Privilege Escalation* osiot ovat osoittautuneet joillekin käyttäjille haasteellisiksi tai työläiksi. Toisaalta yhteinen näkemys tuntuu olevan, että polun suorittaminen takaa riittävän tieto- ja taitotason suorittajille. Polun rakennetta, omatahtista suoritusmahdollisuutta sekä joustavuutta kiitellään laajasti. Yleisen tietoturvaluustietoisuuden edistämisen tutkimisen kannalta onkin mielenkiintoista, miten kommentteista nousee esille esimerkiksi *social engineering* roolin tärkeyden ymmärryksen kasvaminen, minkä voi tulkita kuvastavan syvällisen ymmärryksen karttumista polkua suorittaessa. Tämän voisi puolestaan tulkita tukevan hyvin tietoturvatietoisuuden kasvamista kyseisen oppimispolun suorittamisen yhteydessä.

Valittu polku koostuu kahdeksasta eri osa-alueesta (*Section* tai *Task*), jotka muodostuvat 38 erillisestä huoneesta tai harjoituksesta. Alustan ilmoittama arvioitu oppimispolun suorittamisaika on 64 tuntia. Oppimispolun yleisinä esitietovaatimuksina pidetään tietojenkäsittelytieteen perusosaamista sekä yleistä ymmärrystä eri tietoturvaluuden osa-alueista. Osa valitun oppimispolun harjoitteista vaatii ”*Premium*”-tilauksen (testauskellä 12 puntaa kuukaudessa). Tässä työssä käytettiin kyseistä, ”*Premium*”-tilausta. Yleisten keskustelufoorumien kommenttien perusteella, *TryHackMe*-alustaa voisi käyttää hyvin myös ilman tilausta. Lisäksi alustasta on tarjolla myös yrityksille suunnattu ”*Business*”-laajuus, jolloin alustan ominaisuudet ovat normaalia ”*Premium*”-tilausta laajemmat. Tällöin voisi esimerkiksi räätälöidä yrityksen käyttöön omia eri moduleista rakennettuja oppimispolkua. Alustan eri tilausten laajuudet on kuvattu alle sivuston oman koonnin perusteella (Kuva 5).

	Free	Premium	Businesses
Personal hackable instances	✓	✓	✓
Hacking challenges	✓	✓	✓
Learning content	Free rooms	Premium rooms	Premium & Business rooms
Full access to learning paths	⊗	✓	✓
Web-based AttackBox & Kali	1 hour a day	Unlimited	Unlimited
Access to Networks	⊗	✓	✓
Faster Machines	⊗	✓	✓
Private OpenVPN Servers	⊗	✓	✓
Private King of the Hill Games	⊗	✓	✓
Custom Learning Paths	⊗	⊗	✓
Advanced Reporting	⊗	⊗	✓
Transferable Licensing	⊗	⊗	✓
Dedicated Customer Success Manager	⊗	⊗	✓

Kuva 5. Eri tilausvaihtoehtojen ominaisuudet TryHackMe-alustalla (tryhackme.com/why-subscribe haettu 24.6.2024).

Alla on esitetty sitaatti tutkijan muistiinpanoista.

Ensivaikutelma alustasta, sekä valitusta oppimispolusta on positiivinen. Erilaisten keskustelufoorumien perusteella alusta soveltuu erittäin hyvin vähemmän kokeneelle käyttäjälle, ja kokemukset alustan käytöstä ovatkin yleisesti positiiviset. Valitun polun arvioitu suoritus-aika on pitkä, eikä tämän kokonaisuuden läpikäyminen yleisenä harjoitteena esim. yrityksessä vaikuta olevan järkevää laajamittaisesti. Odotan mielenkiinnolla sitä mitä oppimispolku tuo tullessaan, ja toivon että siitä nousee esille joitakin erityisen mielenkiintoisia tai muuten yleistettäviä kokonaisuuksia, joita voisi erillisinä harjoitteina käyttää laajamittaisemmin.

3.4 Murtautumistestauksen harjoittelu valitulla alustalla

Tässä kappaleessa esitetään tutkijan tekemän refleктоivan tutkimuksen tulokset. Ensimmäisessä aliluvussa käsitellään harjoitusjärjestelyä yleisesti, minkä jälkeen käsitellään jokainen valitun oppimispolun osa-alue omana kokonaisuutenaan.

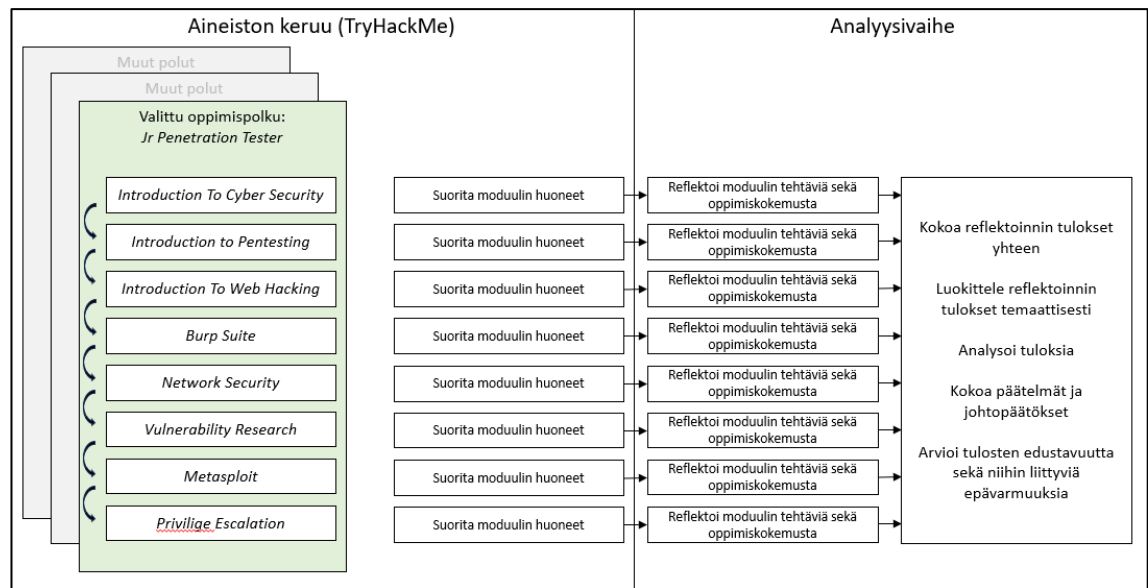
3.4.1 Harjoittelunjärjestelyn kuvaus

Yksi keino murtautumistestauksen opetteluun on harjoitella testausta simuloituilla verkkopohjaisilla murtautumistestausalustoilla. Tässä luvussa tarkastellaan, miten tällainen käyttöympäristö soveltuu murtautumistestauksen harjoitteluun, ja arvioidaan miten mahdollisesti kertyvä ymmärrys tietoturvasta voi lisätä yleisemmin tietoturvallisuutta yhteisössä tai yrityksessä.

Aluksi tutustutaan alustaan TryHackMe, testataan alustaa sekä arvioidaan mielikuvaa alustan soveltuvuudesta murtautumistestauksen harjoitteluun sekä tietoturvaluustietoisuuden parantamiseen ennen varsinaista harjoittelua.

Tämän jälkeen kuvataan harjoittelua valitussa järjestelmässä sekä reflektoidaan kokemuksia harjoittelun etenemisestä. Reflektoidaan tutkimuksen rinnalla tehdään kokeellinen vertaileva tutkimus, jossa koostetaan muiden käyttäjien kommenteista tekoälyavusteisesti vaihtoehtoiset näkemykset tutkimuskysymyksiin. Kolmannessa osiossa koostetaan jälkiarviona käyttäjän omat sekä muista tietolähteistä koostetut kokemukset ja kootaan laadullisen tutkimuksen tulokset yhteen analyysivaihetta varten.

Valittu oppimispolku koostuu kahdeksasta osa-alueesta, jotka esitellään ja käsitellään tässä työssä omina alalukuinaan. Harjoittelun aikana suorittaen oppimispolun osa-alueet (moduulit) oppimispolun tarjoamassa järjestyksessä yksitellen. Jokaisen moduulin suorituksen aikana kerättiin aineistoa (kokemukset) huoneen suorittamisesta. Kaikkien osa-alueiden suorittamisen jälkeen koottiin puolestaan kokemukset yhteen sekä analysoitiin näitä temaattisen analyysin avulla. Lopuksi näistä muodostettiin päätelmät ja johtopäätökset, joita verrattiin myös vastaavaan analyysiin muiden käyttäjien kokemuksista. Aineiston keruun prosessi on esitetty kuvassa alla (Kuva 6).



Kuva 6. Refleктоivan tutkimuksen aineistonkeruu ja analyysi, prosessikuvaus

Seuraavissa luvuissa esitetään oppimispolun sisältö sekä käyttäjän kokemukset harjoituksista osa-alueittain (moduuli).

3.4.1.1 Osa 1: *Introduction to Cyber Security*

Ensimmäinen osio käsitteli tietoturvaä yleisesti esitellen erikseen hyökkäävän sekä puolustavan tietoturvan periaatteet käytännön erimerkin avulla. Hyökkäävän tietoturvan harjoituksessa tutustuttiin piilotetun sivuston tunnusteluun *gobuster* työkalulla. Puolustavan tietoturvan harjoituksessa puolestaan simuloitiin yksinkertaista SOC-tiimin (*Security Operations Center*) tekemää operaatiotta, käyttäen SIEM-järjestelmää (*Security Information and Event Management*). Lisäksi osiossa tutustuttiin lyhyesti tietoturva-alan erilaisiin työnkuviin.

Alla on esitetty sitaatti tutkijan muistiinpanoista.

Harjoitukset olivat selkeitä, helposti ymmärrettäviä sekä toteutettavia. Sisällöltään nämä eivät tarjonneet erityisesti mitään uutta käyttäjälle, mutta saivat toki pohtimaan vastaavien tapausten soveltuvuutta käytännön elämään. Arvioisin osion sopivan hyvin kaikille käyttäjille yleiseen aihepiiriin tutustumiseen sekä riskipohjaisen

ajattelun herättelyyn sekä yleiseksi harjoitukseksi kokonaisuuteen sekä metodologiaan tutustumiseen.

3.4.1.2 Osa 2: *Introduction to Pentesting*

Toinen osio käsitteli murtautumistestauksen (Pentesting) perusteita, siihen liittyviä eettisiä periaatteita sekä sääntöjä, yleisesti käytettyä prosessia ja menetelmiä. Osion harjoitus simuloi yksinkertaista murtautumistestaustilannetta, tavoitteena testata järjestelmää yleisen prosessin mukaisesti.

Lisäksi toisessa osiossa käsiteltiin tietoturvan (*information security*) perusperiaatteita keskittyen erityisesti datan suojaamiseen sekä tietoturvan ja tiedonsuojaamisen perusperiaatteisiin sekä uhkamallinnukseen ja tapahtumiin reagoimiseen. Ensimmäisen vaiheen harjoituksessa visualisoitiin hyvin yleisellä tasolla tietoliikennettä testauksen aikana. Toinen vaihe puolestaan koostui pääosin tekstimuotoisesta tiedosta, sekä usein kysytyistä kysymyksistä tämän pohjalta.

Alla on esitetty sitaatti tutkijan muistiinpanoista.

Osio oli selkeä ja lähestyi sisällöltään enemmän ja enemmän aihepiiriin erityispiirteitä. Osio antoi selkeän kuvan yleisestä prosessista ja sisälsi selkeän prosessikuvauksen murtautumistestaukseen, mikä oli hyvä. Testausosiossa painottuivat perusasiat, kuten lupien laajuuden (scopen) sekä sääntöjen määrittäminen. Tarkempi testaus, kuten tiedonkeruu, skannaus ja heikkouksien hyödyntäminen käsiteltiin hyvin pinnallisella tasolla. Yleisesti pidin tätä ihan hyvänä yleiskuvauksena. Jos aihe on vieras, tämä on nopea tapa käydä läpi yleiset periaatteet. Osion soveltuvuus laajempaan käyttöön on kohtalaisen hyvä: asiaa entuudestaan tuntevat tuskin tästä mitään uutta saavat, mutta jos murtautumistestaus ei ole entuudestaan tuttua, antaa tämä osio hyvin nopean yleiskuvan aiheeseen.

3.4.1.3 Osa 3: *Introduction to Web Hacking*

Osiossa perehdyttiin verkkosovelluksen turvallisuushiin sekä niiden heikkouksien hyväksikäyttämiseen. Osio oli polun ensimmäinen laajempi kokonaisuus, joka sisälsi useita käytännön harjoitteita. Osiossa oli kahdeksan eri huonetta,

jotka käsittelivät muun muassa verkkosovelluksen tutkimista selaimen kehittäjätyökalujen avulla, sovelluksen ominaisuuksiin perehtymistä esimerkiksi avoimen tietolähteen tiedustelun avulla tai esimerkiksi analysoimalla sivun rakennetta tai siinä käytettyjä komponentteja. Lisäksi tutustuttiin eri menetelmiin, joilla käyttäjän varmistus on mahdollista ohittaa sekä erilaisiin haavoittuvuuksiin.

Alla on esitetty sitaatti tutkijan muistiinpanoista.

Osion huoneissa oli useita käytännön harjoituksia, joiden rakenteet vaihtelivat hyvin paljon avustetuista (seuraa perässä) muutamiin haasteellisiin, joissa itse jouduin käyttämään erilaisia internet tietolähteitä apunani. Osiot olivat yleisesti ottaen mielenkiintoisia sekä kohtalaisen haastavia. Osio oli mielestäni hyvin laaja ja ajankäytöllisesti työläs. Osassa harjoituksista erityisesti Burp Suiten käyttäminen ratkaisi ongelman (tai ainakin helpotti ratkaisemista), mikä oli siinä mielessä erikoista, että itse työkaluun tutustuttiin vasta seuraavassa osiossa. Lisäksi osassa osioista oli paljon tekstimuotoista (lukeminen) asiaan perehtymistä verrattuna käytännön harjoitteiden määrään. Mielestäni käytännön harjoitteita olisi voinut olla enemmän. Toisaalta "seuraa perässä" tehtävät olivat siinä mielessä hyviä, että ne demonstroivat hyvin tapauksia, joiden tekeminen harjoitusmuotoisena olisi voinut olla hyvinkin hankalaa.

3.4.1.4 Osa 4: *Burp Suite*

Tässä osiossa perehdyttiin nimensä mukaisesti Burp Suite ohjelmaan, sen ominaisuuksiin sekä käyttöön osana murtautumistestausta. Erityisesti perehdyttiin *Repeater* ja *Intruder* työkaluihin sekä käytiin pikaisesti läpi muita, vähemmän tunnettuja ominaisuuksia; *Decoder*, *Comparer*, *Sequencer*, ja *Organizer*.

Alla on esitetty sitaatti tutkijan muistiinpanoista.

Yleisesti ottaen osio oli mielenkiintoinen ja hyvin kasattu. Perusosio sisälsi paljon suhteellisen helppoja, käytännönläheisiä esimerkkejä, kun taas syvemmälle ohjelmaan sukeltavissa oli useampia haasteellisia tehtäviä, jotka olivat hyvin opettavaisia, mutta jotka vaativat syvällistä paneutumista sekä intensiivisempää ajankäyttöä. Osassa tehtävistä oli lisäksi mahdollista toteuttaa tehtävät joko sokeana, tai avustettuna versiona riippuen tekijän mielenkiinnosta osiota kohtaan sekä pohjatiedoista. Mielestäni tämä on hyvä järjestely, koska

se mahdollistaa erilaisin taustoin ja kiinnostuksenkohtein mielekkään suorittamisen.

3.4.1.5 Osa 5: Network Security

Osiossa tutustuttiin tiedusteluun, erityisesti Nmap työkalun käyttöön sekä yleisesti eri protokolliin ja niihin liitettäviin hyökkäysvektoreihin. Tiedustelua käsiteltiin erikseen aktiivisen (tietoverkon kautta) ja passiivisen tiedustelun kautta (esimerkiksi julkiset tietueet ja muu netissä saatavilla oleva materiaali).

Osio käsitteli mm. TCP- ja UDP-yhteyksien skannauksia, sekä FTP-, POP3-, SMTP-, ja IMAP-protokollia. Lisäksi käsiteltiin salasanoja ja yleisesti tekstimuotoisen tietoliikenteen riskejä ja niiden mitigointia. Osion päätteeksi oli kattava haastetehtävä, jossa järjestelmästä pyrittiin kaivamaan erilaista tietueita.

Alla on esitetty muutama sitaatti tutkijan muistiinpanoista.

Mielestäni nmap-työkalun perusteita kattava osio oli jossain määrin turhan yksinkertainen tai helppo, mutta sinänsä osio oli jokseenkin nopea suorittaa. Ehkä tämä olisi toiselle yleisölle mielenkiintoinen kokonaisuus.

Yleisesti osiossa oli monia hyvinkin mielenkiintoisia kohtia, joita oli helpohko seurata. Osion tekeminen vaati jonkin verran pohdintaa, mikä lisäsi mielestäni kiinnostavuutta. Mielestäni osio oli hyvä kuvaus aiheesta eikä se ollut liian työläs.

Osiossa oli hyvin eroteltu mahdollisuus seurata ohjeiden avulla käytännön harjoitteita, tai oma-aloitteisesti yrittää niiden suorittamista, mikä on hyvä asia kun mietitään osion soveltuvuutta eri käyttäjille. Erityisesti osion lopputehtävä, "Net Sec Challenge", oli erittäin opettavainen laajan käytännön harjoittelun vuoksi.

3.4.1.6 Osa 6: Vulnerability Research

Vulnerability Research -osiossa tarkasteltiin yleisesti järjestelmien heikkouksia, sekä perehdyttiin tarkastelemaan minkälaisia nämä yleisesti ovat ja miten eri heikkouksia mm. arvotetaan (CVSS & VPR) niiden muodostaman uhan suhteen.

Eri arvotusmenetelmien avulla käytiin läpi priorisointia sekä toimenpiteiden kohdentamista kaikkein tärkeimpien korjaavien toimien tekemiseen mahdollisimman nopeasti. Lisäksi perehdyttiin työkaluihin, tekniikoihin ja resursseihin, joiden avulla heikkouksia voidaan pyrkiä hyödyntämään.

Osion päätteeksi oli lopputehtävä: Vulnerability Capstone, jossa harjoiteltiin järjestelmän heikkouden tunnistamista sekä hyödyntämistä käytännössä.

Alla on esitetty sitaatti tutkijan muistiinpanoista.

Teoria osio oli mielestäni ihan hyvä, ei liian haasteellinen. Erityisesti haastetehtävä oli hyvä, vaikkakin suhteellisen vaikea... ei millään mene laskennalliseen 20 min aikaikkunaan. Arvioisin että tehtäväkokonaisuuden kunnollinen ymmärtäminen vaatii merkittävästi enemmän aikaa kuin osioille on laskennallisesti arvioitu. Kuitenkin harjoitustehtävä oli erittäin opettavainen ja hyvin käytännöllinen. Tietoturvatietoisuuden lisäämisen näkökulmasta tämä harjoitus on erityisesti opettavainen siinä kuinka helppoa erilaisten heikkouksien hyödyntäminen voi olla korostaessaan huolellisen toteutuksen sekä kehitysprosessien noudattamisen tärkeyttä.

3.4.1.7 Osa 7: Metasploit

Metasploit-moduulissa tutustuttiin nimensä mukaisesti kyseisen työkalun toimintaan, ominaisuuksiin sekä käyttömahdollisuuksiin. Osio oli jaettu kolmeen osioon: tutustuminen työkaluun yleisesti, työkalun käyttöön murtautumistestauksessa sekä Meterpreter-toiminnallisuuden käyttämiseen esimerkiksi murtautumistestausyrityksen piilotteluun sekä havaitsemisen välttelyyn. Osion lopuksi oli haastetehtävä, jossa tavoitteena oli murtautua järjestelmään ja kerätä sieltä tietoa.

Alla on esitetty sitaatti tukijan muistiinpanoista.

Osio oli mielestäni hyvä yleinen tutustuminen työkaluun, ja luontevasti osiossa hyödynnettiin aikaisempien osa-alueiden asioita. Teorettisempi osio oli suhteellisen helposti lähestyttävä, ja oppimista tukivat selkeät esimerkkitehtävät. Metasploit osion ”parasta antia” oli mielestäni haastetehtävä, jossa korostui tekemällä oppiminen.

Joskin on erikseen mainittava, että ilman erillistä tutustumista ohjelman ominaisuuksiin ja aiheisiin tarjotun opiskelumateriaalin ulkopuolisin lähteitten avulla haastetehtävä olisi tuskin itseltäni onnistunut, mutta onneksi on internet apuna.

3.4.1.8 Osa 8: Privilege Escalation

Osiossa tutustuttiin aluksi "shell"-käyttöympäristöön ja siihen, kuinka näitä voi lähettää kohteesta sekä vastaanottaa kohteeseen osana murtautumistestausta. Osiossa tutustuttiin mm. työkaluihin Netcat, Socat, Metasploit multi/hander sekä Msfvenom.

Tämän jälkeen perehdyttiin erikseen Linux sekä Windows-järjestelmissä toteuttavaan oikeuksien korottamiseen järjestelmien yleisten eroavaisuuksien ja ominaisuuksien sekä näiden hyödyntämistapojen kautta.

Olla on esitetty sitaatteja tutkijan muistiinpanoista.

Linux-osion huoneessa oli reilusti luettavaa, ja käytännön esimerkkejä joita pystyi tekemään materiaalin mukana. Huone oli mielestäni hyvä, ja tarjosi laajan mahdollisuuden kokeilla ja tutustua esiteltyihin menetelmiin. Huone simuloi hyvin todellista joskin rajatusti suojattua ympäristöä.

Windows-osion huone oli mielestäni pitkä, työläs ja haastava, joskin opettavainen. Lisäksi on hyvä huomata kuten harjoituksessakin mainitaan, että esitetyt tekniikat koskettavat pääosin CTF-pelejä tai muita vastaavia harjoituksia paremmin kuin tosielämän tilannetta.

Eryityisesti mieleeni jäi, että on tärkeintä tiedostaa, että vastaavat tavat ovat mahdollisia, ei niinkään harjoiteltujen teknisten yksityiskohden kautta, vaan enemmänkin yleisesti tavalla tai toisella riippuen tilanteesta

3.5 Muiden käyttäjien kokemukset murtautumistestauksen harjoittelusta valitulla alustalla

Tässä kappaleessa käsitellään muiden käyttäjien kokemuksia vastaavasta alustasta sekä oppimispolusta.

3.5.1 Yleiset kokemukset oppimispolusta

Tämä aliluku on koostettu kappaleessa 2.2.2 esitetyn menetelmän mukaisesti, perustuen sosiaalisen median lähteisiin ja keskustelupalstoilla esitettyihin näkemyksiin (Reddit-keskustelu, 2022; Espinosa, 2023; Hon, 2023).

Junior Penetration Tester-polku koetaan yleisesti monipuoliseksi kokonaisuudeksi, joka käsittelee murtautumistestauksen yleiset periaatteet, työkalut ja menetelmät laaja-alaisesti. Polku keskittyy reaali maailman skenaarioihin, joiden voidaan nähdä tehokkaasti valmentavan opiskelijoita tosielämän tietoturva haasteisiin.

Eryteisesti oppimispolun soveltuvuutta tietoturvatietoisuuden kasvattamiseen arvioidaan sen kattavuuden ja monipuolisuuden sekä monipuolisuutensa kautta sekä käytännön harjoitusten kautta. Nämä harjoitukset mahdollistavat teoreettisen ymmärryksen soveltamisen käytännön tosielämän haasteisiin.

Eryteisesti polun monipuolisuuden nähdään parantavan tietoturvatietoisuutta.

3.5.1.1 Introduction to cyber security

Tämä aliluku on koostettu kappaleessa 2.2.2 esitetyn menetelmän mukaisesti, perustuen lähteisiin (CyberEyes, 2022; Fireshark, 2023).

Introduction to cyber security-moduulin olevan suoraan sovellettavissa todellisen maailman tilanteisiin, sillä siinä yhdistyvät todellisuutta mukailevat simulatiot sekä käytännön harjoittelu erilaisten soveltavien harjoitusten kautta. Moduulissa yhdistyvät käytännön työkalujen käyttö sekä yleinen hyökkäävän sekä puolustavan tietoturvan yhteispeli. Näiden kautta puhuja esittää, että opiskelijan kyky tunnistaa ja hallita erilaisia heikkouksia paranee. Myös perustavanlaatuisen ymmärryksen turvallisista (suojatuista) tiedonsiirtomenetelmistä nähdään arvokkaaksi.

Yleisesti puhuja esittää, että monipuolinen tietoturvakoulutus soveltuu hyvin tietoturvatietoisuuden ja yleisen varautumisen edistämiseen.

3.5.1.2 Introduction to Pentesting

Tämä aliluku on koostettu kappaleessa 2.2.2 esitetyn menetelmän mukaisesti, perustuen lähteisiin Rosen (2023a) sekä Shaunna's Workshop (2022).

Kommentoijan mielestä osio tukee tietoturvatietoisuuden parantamista erityisesti käsittelemällä murtautumistestauksen peruseriaatteita, kuten viitekehyksiä ja metodeja sekä yleisesti murtautumistestauksen roolia osana kokonaispuolustusta. Lisäksi kommentoijan mukaan on arvokasta tiedostaa testaukseen liittyvät juridiset sekä eettiset seikat. Myös tosielämää simuloivien harjoitusten voidaan ajatella tukevan yleistä tietoturvatietoisuuden kehittymistä.

Yleisesti puhujan mielestä moduuli parantaa tietoturvatietoisuuden kehittymistä monipuolisuudellaan sekä käytännön esimerkkien kautta. Moduulin koetaan yhdistävän hyvin teoreettinen ymmärrys käytännön sovellutuksiin sekä näiden kautta tosielämän tietoturva haasteisiin.

3.5.1.3 Introduction to Web hacking

Tämä aliluku on koostettu kappaleessa 2.2.2 esitetyn menetelmän mukaisesti, perustuen Palaez (2022) näkemyksiin.

Arvioija kuvailee Introduction to Web hacking osiota muutaman kriittisen teeman kautta. Arvioijalla oli osiossa merkittäviä teknisiä haasteita, jotka johtivat turhautumisiin. Erityisesti nämä johtuivat teknisestä kompleksisuudesta tehtävässä. Toisella esimerkiksi että *"I am going to lose my mind"* ('Menetän hermoni').

Toisaalta arvioija tunnistaa myös harjoitusten opettavaisen arvon todeten muun muassa, että harjoitus mahdollistaa aikaisemman osaamisen (arvioijan kohdalla

tilastotieteestä) yhdistämisen tietoturvallisuuden teoriaan ja käytännön konsepteihin, jonka pohjalta voitaneen tulkita tietoturvatietoisuuden kehittyvän osana harjoitusta. Myös käytännönläheiset tosielämän esimerkit nostetaan tekstissä esille hyvänä valmentavana mallina tosielämän tietoturva haasteisiin valmistautumisessa.

Koetuista haasteista huolimatta arvioija pitää kokemustaan positiivisena, vaikkakin harjoitusosio olikin hänelle hyvin aikaa vievä sekä haastava. Yleisesti arvioija toteaa, että tietoturvan harjoittelu voi olla haasteellista sekä aikaa vievää, mutta samalla avainasemassa vahvistamassa teoreettisen tiedon ja käytännön taitojen yhdistämistä.

3.5.1.4 Burp Suite

Tämä aliluku on koostettu kappaleessa 2.2.2 esitetyn menetelmän mukaisesti, perustuen sosiaalisessa mediassa käyttäjän Rosen jaettuihin kokemuksiin (Rosen: 2023b, 2023c, 2023d, 2023e, 2023f)

Osion Burp Suite koettiin olevan hyvin käytännönläheinen (*hands-on*), sekä kattavan laajasti erilaiset työkalut ja työkalujen ominaisuudet. Osion kuvataan ohjaavan opiskelijaa selkeästi läpi erilaisia toiminnallisuuksia esittelevien harjoitusten. Harjoitusten todetaan kehittävän ongelmanratkaisua sekä kriittistä ajattelua interaktiivisten tehtävien sekä skenaarioiden avulla. Harjoitusten kuvataan jopa kehittävän ymmärrystä tietoturvallisuuden pohjimmaisten haasteiden ja prosessien osalta.

Käytännön elämää simuloivien harjoitusten todetaan olevan avainasemassa harjoituksen tehokkuudessa. Osion harjoitusten todetaan yleisesti myös olevan hyvinkin tarkasti opastettuja, vaikka osion jotkin harjoitukset voivat silti osoittautua haastaviksi aloittelijoille. Arvioijan mielestä tätä haastetta voisi kehittää tarjoamalla yksinkertaistettuja selityksiä sekä laajempaa lisämateriaalia tietyistä osa-alueista. Myös laajemman tosielämän kontekstin avaaminen voisi tukea yleistä ymmärryksen kehittymistä.

Yleisesti osiota pidetään tehokkaana tapana parantaa tietoturvatietoisuutta käytännön esimerkkien ja harjoitusten avulla. Toisaalta osiota voisi kehittää erityisesti kokemattomampien opiskelijoiden tukemiseksi tarjoamalla erillistä lisämateriaalia nykyistä laajemmin.

3.5.1.5 Network Security

Tämä aliluku on koostettu kappaleessa 2.2.2 esitetyn menetelmän mukaisesti perustuen käyttäjän Rosen kokemuksiin (2023g, 2023h, 2023i, 2023j, 2023k, 2023l, 2023m, 2023n, 2023o).

Teksti (puhuja) esittää *Network Security*-osion tukevan tietoturvatietoisuuden kasvattamista erityisesti erilaisten käytännön taitojen kehittämisen sekä työkalujen toiminnan opettelun kautta. Osion kuvataan kehittävän erityisesti passiivista tiedustelua, aktiivista tiedustelua, erilaisten hyökkäystapojen ja poikkeamien hallinta strategioita.

Näiden kautta puhuja arvioi mm. seuraavien taitojen kehittyvän merkittävästi; heikkouksien tunnistaminen sekä hallinta (mitigation), turvallinen tiedonsiirto ja kommunikaatio.

Arvioija pitää tosielämän esimerkkejä tärkeänä osana moduulia ja arvioi näiden tukevan laajemman organisaatiotason tietoturvan ymmärrystä sekä parantamista. Lisäksi harjoitteiden arvioidaan tukevan itsenäisen ongelmaratkaisun kehittymistä.

Osion kerrotaan tarjoavan selkeää vaiheittaista opastusta aihepiirin harjoitukseen, joka tukee opiskelijoiden ymmärrystä sekä teknisissä että konseptuaalisissa tietoturvaasioissa. Arvioija esittää vahvan uskomuksensa siihen, että harjoitus tukee yleisesti tietoturvatietoisuuden kehittymistä.

Toisaalta puhuja nostaa esille sen, että kyseinen harjoitus käsittelee pitkälle erikoistunutta osa-aluetta, joka vaatii osin syvällistä teknistä ymmärrystä, joten

harjoituksen soveltuvuus tietoturvan parantamiseen koskettaa erityisesti tietoliikenne ja tietoturva-alan ammattilaisia. Vähemmän teknisesti valveutuneen yleisön osalta puhuja mainitsee mahdollisen tarpeen harjoituskokonaisuuden tarkentamiseen niin, että se olisi helpommin lähestyttävä sekä sisällöltään paremmin sopiva.

Yleisesti osion arvioidaan olevan tasapainoinen kokonaisuus teoreettisen tiedon kehittämisen sekä käytännön harjoitteiden välillä. Moduulin arvioidaan myös kykenevän hyvin luomaan realistisen kokonaiskuvan käytännön tieturvahaasteista sekä niiden käsittelemisestä organisaatiolle järkevällä tavalla, varsinkin parhaiden käytänteiden esittelyn ja käsittelyn kautta.

3.5.1.6 Vulnerability Research

Tämä aliluku on koostettu kappaleessa 2.2.2 esitetyn menetelmän mukaisesti, perustuen käyttäjän Rosen kokemuksiin (2023p, 2023q, 2023r).

Puhujan mukaan osio on tehokas työkalu tietoturvatietoisuuden lisäämiseksi. Erityisesti käytännön elämän harjoitukset sekä viitekehyksien että työkalujen käyttö ja yhteensovitus on hänen mielestään arvokasta sisältöä. Puhuja esittää näkemyksen, että käytännön harjoitteiden kautta lisääntyy yleinen tiedostaminen ja valmius tietoturvasta ja -poikkeamista. Osion nähdään tukevan hyvin tilanteita, joissa suorittaja tarvitsee erillistä tukea esimerkiksi teknisten haasteiden selvittämisessä. Erityisesti puhuja pitää osiota soveltuvana tietoteknisellä alalla toimiville henkilöille. Toisaalta puheesta on tulkittavissa, että osion soveltuvuus henkilöille, joilla ei ole vahvaa osaamista tietotekniikasta entuudestaan, on heikko.

3.5.1.7 Metasploit

Tämä aliluku on koostettu kappaleessa 2.2.2 esitetyn menetelmän mukaisesti, perustuen käyttäjän Rosen kokemuksiin (2023s, 2023t, 2023u).

Puhujan näkemyksen mukaan tämä harjoituskokonaisuus soveltuu hyvin tietoturvatietoisuuden lisäämiseen. Erityisesti yksityiskohtainen tekninen lähestymistapa sekä käytännön tehtäviin keskittyvät harjoitteet tukevat käyttäjän ymmärryksen sekä käytännön osaamisen kehittymistä. Erityisen positiivisesti puhuja suhtautuu tosielämään tilanteita simuloivien harjoitteiden käytännönläheiseen soveltamiseen. Puhuja esittää myös luottamuksensa siihen, että ohjelman joustavuus ja mukautettavuus tukevat oppimismuotoa.

3.5.1.8 Privilege Escalation

Tämä aliluku on koostettu kappaleessa 2.2.2 esitetyn menetelmän mukaisesti, perustuen käyttäjien Rosen (2023v) sekä Hamdan (2021; 2022) kokemuksiin.

Puhujan näkemyksen mukaan harjoitusosiossa korostuvat erityisesti käytännön harjoitteet, teknisten taitojen kehitys, yleinen ongelmanratkaisu sekä kriittinen ajattelu. Tietoturvatietoisuuden parantamisen nähdessä erityisesti syntyvän käytännön harjoitteiden kautta. Toisaalta parempiin tuloksiin pääsemiseksi ehdotetaan että harjoittelun tulisi tasapainottaa nykyistä paremmin teknisten taitojen linkittymistä laajempaan kokonaisuuteen, kuten organisatorisen tason vaikutuksia poikkeamatilanteissa, sekä linkittymistä turvallisuusstrategiaan. Lisäksi puhuja nostaa esille tarpeen aloittelijoille soveltuvamman toiminnallisen sisällön lisäämisen, jotta harjoitus olisi soveltuvampi laajemmalle yleisölle. Esimerkkejä tästä voisivat olla tietoturvan peruseriaatteiden läpikäyminen ja linkittäminen osaksi harjoitteita sekä harjoiteltujen tekniikoiden todellinen merkittävyys laajemmassa kontekstissa.

Puhuja korostaa myös sitä, että materiaali voisi käsitellä nykyistä laajemmin kuinka esitetyn kaltaisia heikkouksia tai hyökkäyksiä vastaan puolustaudutaan esimerkiksi turvallisuusohjeistusten kehittämisen sekä laajemman turvallisuus-kulttuurin jalkauttamisen ja kehittämisen avulla.

Yleisesti harjoituskokonaisuutta pidetään hyvin käytäntöön soveltuvana, erityisesti käytännön harjoitteiden kautta. Vastaavasti harjoituskokonaisuuden vaikuttavuutta voidaan arvioida sen mukaan kuinka hyvin kokonaisuus nähdään olevan suunniteltu ja kuinka sen nähdään keskittyvän oikeisiin asioihin.

4 Tulosten arviointi

Tämä kappale käsittelee kokemukseen perustuvan laadullisen tutkimuksen tulosten käsittelyä.

4.1 Omien kokemusten arviointi

Omien kokemusten arviointi aloitettiin koodaamalla alustavilla koodeilla kokemusten perusteella kerätyt huomiot ja mielipiteet. Alustavan koodauksen perusteella tunnistettiin yleisemmät kommentteja kuvaavat teemat, jotka aineiston analysoinnissa nousivat esille. Tunnistetut teemat olivat; harjoitusmateriaalin lähestyttävyyys, käytännön tekeminen, mukautuvuus, harjoituksen rakenne, opitun soveltaminen sekä harjoitusten työläys.

Harjoitusmateriaalin lähestyttävyyys korostui erityisesti harjoituskokonaisuuden ensimmäisissä neljässä osiossa. Tähän teemaan on kuvattu erityisesti kommentteja, jotka kuvaavat niitä huomioita, joiden on tulkittu kuvaavan kokemuksia, jotka liittyvät materiaaliin ja osioihin, jotka ovat helposti ymmärrettävissä ja suoritettavissa hyvinkin vähäisellä taustaymmärryksellä tarkemmasta teknisestä kokonaisuudesta. Esimerkkejä kokemuksista ovat mm.

Harjoitukset olivat selkeitä, helposti ymmärrettäviä sekä toteutettavia

Osio sisälsi paljon suhteellisen helppoja, käytännönläheisiä esimerkkejä

Käytännön tekemisen teema korostui puolestaan erityisesti osioissa 3-7. Teemaan on liitetty kommentit, jotka kuvaavat erityisesti konkreettista tekemistä, joko "seuraa perässä"-mallilla, tai vastaavasti itsenäisten harjoitusten kautta.

Tämä teema koostui monessa kohtaa refleктоijan kokemuksiä. Esimerkkejä kommenteista poimituista teemaa kuvaavista huomioista on esitetty alla.

Toisaalta "seuraa perässä" tehtävät olivat siinä mielessä hyviä, että ne demonstroivat hyvin tapauksia joiden tekeminen harjoitusmuotoisena olisi voinut olla hyvinkin hankalaa.

Erityisesti osion lopputehtävä, "Net Sec Challenge", oli erittäin opettavainen laajan käytännön harjoittelun vuoksi.

Kuitenkin harjoitustehtävä oli erittäin opettavainen ja hyvin käytännöllinen.

Metasploit osion parasta antia oli mielestäni haastetehtävä, jossa korostui tekemällä oppiminen

Mukautuvuus-teeman nähtiin kuvaavan osioiden soveltuvuutta eritasoisille tai eri asioista erityisesti kiinnostuneille henkilöille. Teemaan kuului mm. kokemuksia harjoitteista, jotka oli mahdollista suorittaa joko itsenäisesti tai vaihtoehtoisesti avustettuna seuraamalla ohjeita. Lisäksi teemaan on sisällytetty kommentteja, jotka kuvastavat refleктоijan tulkintaa tai pohdintaa liittyen aihealueen mahdolliseen soveltumiseen laajalle yleisölle. Esimerkkejä teemaan liittyvistä kommenteista on esitetty alla:

Osiossa oli hyvin eroteltu mahdollisuus seurata ohjeiden avulla käytännön harjoitteita tai oma-aloitteisesti yrittää niiden suorittamista, mikä on hyvä asia kun mietitään osion soveltuvuutta eri käyttäjille

Osion huoneessa oli reilusti luettavaa ja käytännön esimerkkejä, joita pystyi tekemään materiaalin mukana. Huone oli mielestäni hyvä ja tarjosi laajan mahdollisuuden kokeilla ja tutustua esiteltyihin menetelmiin

Tehtävistä oli lisäksi mahdollista toteuttaa ne joko sokeana tai avustettuna versiona riippuen tekijän mielenkiinnosta osiota kohtaan sekä pohjatiedoista

Mielestäni tämä on hyvä järjestely, koska se mahdollistaa erilaisin taustoin ja kiinnostuksenkohtein mielekkään suorittamisen.

Rakenne-teemaan on puolestaan koettu kuuluvaksi kommentit, joiden nähtiin kuvastavan yleisesti harjoituskokonaisuuden rakennetta sekä eri osa-alueiden linkittymistä toisiinsa. Teemaan sisältyviä kommentteja olivat esimerkiksi:

Erityisesti Burp Suiten käyttäminen ratkaisi ongelman (tai ainakin helpotti ratkaisemista), mikä oli siinä mielessä erikoista että itse työkaluun tutustuttiin vasta seuraavassa osiossa.

Osio oli mielestäni hyvä yleinen tutustuminen työkaluun, ja luontevasti osiossa hyödynnettiin aikaisempien osa-alueiden asioita

Soveltaminen laajemmin -teemaan on puolestaan yhdistetty kommentit, jotka kuvastavat harjoitusten ja harjoittelun linkitystä laajempaan tietoturvallisuuden kehittämiseen tai vastaavasti tietoturvatietoisuuden kehittämiseen. Teemaan on sisällytetty myös osiot, joiden nähtiin esimerkiksi simuloivan todellisia tapauksia tai vastaavia esimerkkejä.

-- yleiseen aihepiiriin tutustumiseen sekä riskipohjaisen ajattelun herättelyyn.

Tietoturvatietoisuuden lisäämisen näkökulmasta tämä harjoitus erityisesti opettavainen siinä kuinka helppoa voi erilaisten heikkouksien hyödyntäminen olla.

Huone simuloi mielestäni hyvin todellista (joskin rajatusti suojattua) ympäristöä.

Erityisesti mieleeni jäi, että on tärkeintä tiedostaa, että vastaavat tavat ovat mahdollisia, ei niinkään harjoiteltujen teknisten yksityiskoh-
tien kautta vaan enemmänkin yleisesti tavalla tai toisella riippuen tilanteesta

-- saivat toki pohtimaan vastaavien tapausten soveltuvuutta käytännön elämään.

Lisäksi tunnistettiin teemat "Työläys" sekä "Yksinkertaisuus", joiden alle on luokiteltu kommentteja, jotka kuvaavat sitä kuinka työläiksi tai haastaviksi harjoitukset koettiin. Teemaan on sisällytetty kommentteja, jotka kuvaavat esimerkiksi erillisten lisämateriaalejen tai tuen tarvetta, tai vastaavasti joissain tapauksissa,

vaikka osioiden asioiden ”itsestään selvyyttä”. Esimerkkejä teeman kommentteista on kuvattuna alla.

-- joissa itse jouduin käyttämään erilaisia internettietolähteitä apunani.

Ilman erillistä tutustumista ominaisuuksiin ja aiheisiin tarjotun opiskelumateriaalin ulkopuolisten lähteiden avulla haastetehtävä olisi tuskin itseltäni onnistunut, mutta onneksi on internet apuna.

-- syvemmälle ohjelmaan sukeltavissa oli useampia haasteellisia tehtäviä, jotka olivat hyvin opettavaisia, mutta jotka vaativat syvällistä paneutumista sekä intensiivisempää ajankäyttöä.

Osion tekeminen vaati jonkin verran pohdintaa, mikä lisäsi mielestäni kiinnostavuutta. Mielestäni osio oli hyvä kuvaus aiheesta, eikä ollut liian työläs.

Teoriaosio oli mielestäni ihan hyvä, ei liian haasteellinen. Erityisesti haastetehtävä oli hyvä, vaikkakin suhteellisen vaikea... ei millään mene laskennalliseen 20 min aikaikkunaan.

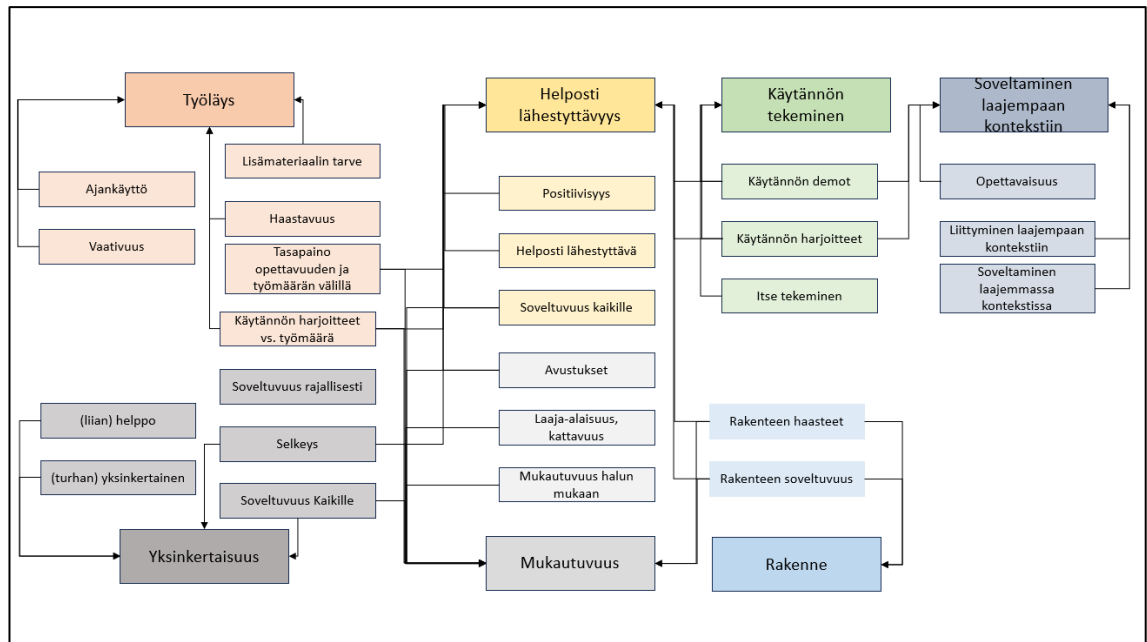
Mielestäni nmap-työkalun perusteita kattava osio oli jossain määrin turhan yksinkertainen tai helppo, mutta sinänsä osio oli jokseenkin nopea suorittaa.

Jos aihe on vieras, tämä on nopea tapa käydä läpi yleiset periaatteet. Osion soveltuvuus laajempaan käyttöön on kohtalaisen hyvä.

-- asiaa entuudestaan tuntevat tuskin tästä mitään uutta saavat.

-- nämä eivät tarjonneet erityisesti mitään uutta käyttäjälle

Refleктоivan tutkimuksen temaattisen koodauksen ja teemoituksen suhdetta on kuvattu alla (Kuva 7).



Kuva 7. Reflektioanalyysin temaattinen kartta, omat kokemukset.

Tutkijan reflektioivan tutkimuksen kommentoissa korostuu merkittävästi positiiviset kokemukset käytännön tekemisen kautta sekä useassa kohtaa myös käytännön tekemisen kautta opitun soveltaminen laajempaan kontekstiin. Lisäksi kommentoissa tuodaan esille materiaalin soveltuvuus monille erilaisille henkilöille sekä harjoitteiden mukautuvuus osaamistason mukaan. Näiden tulkintojen perusteella voidaan vetää johtopäätös harjoittelumenetelmän soveltavuudesta yleisesti tietoturvallisuuden ja tietoturvan parantamiseen.

Toisaalta oppimispolun rakenteen ja materiaalin haasteita kommentoitiin myös. Kehitysehdotuksina näiden haasteiden ratkaisemiseen esitettiin kohtalaisen helposti toteutettavia ratkaisuja, joskin helppous on tilannekohtaista. On tulkittavissa, että tarjoamalla tämän oppimispolun materiaalin lisäksi erillistä lisämateriaalia sekä tarkemman suoritusohjeen oppimispolulle voitaisiin tämän harjoittelumuodon käyttöönottoa esimerkiksi yrityksessä sujuvoittaa suhteellisen pienellä lisätyömäärällä. Näiden tulkintojen perusteella voidaankin ajatella, että materiaali sinänsä sopii tietoturvallisuuden ja tietoturvan parantamiseen mutta sujuva käyttöönotto organisaatiossa vaatii jonkin verran lisävalmisteluja, mikä osin heikentää menetelmän houkuttelevuutta.

Lisäksi joissakin kommenteissa nousi esille harjoitusten työläys sekä vaativuus, mikä omalta osaltaan rajoittaa harjoittelumenetelmän käyttöä laajamittaisesti. Lisäksi, kun huomioidaan että tutkija on taustaltaan valmistumaisillaan oleva tietoliikennetekniikan insinööri, voi näiden työläyteen ja haastavuuteen viittaavien kokemusten arvioida olevan merkittävästi suurempia, jos harjoittelijana olisi esimerkiksi johonkin muuhun alaan erikoistunut insinööri tai tradenomi. Yleistettynä tulkintana voisikin esittää, että vaikka harjoittelumenetelmä voi olla joissain tapauksissa toimiva, tulisi harjoitusmenetelmän soveltuvuus yksilötasolla miettiä hyvin tarkkaan ennen tällaisen menetelmän käyttöönottoa.

4.2 Muiden käyttäjien kokemukset

Muiden käyttäjien kokemusten arviointi aloitettiin koodaamalla alustavilla koodaamilla kerätyt huomiot ja mielipiteet. Alustavan koodauksen perusteella tunnistettiin yleisemmät kommentteja kuvaavat teemat, jotka aineiston analysoinnissa nousivat esille. Temaattisen analyysin pohjalta johdettiin luokittelun mukaisesti yleiset tulkinnat muiden käyttäjien kokemusten pohjalta aineiston soveltuvuudesta tietoturvatietoisuuden lisäämiseksi.

Aineistossa esiintyvät kommentit (koodit) voidaan luokitella yleisesti kolmeen pääkategoriaan; soveltuvuus, soveltaminen ja käytännön harjoittelu. Osioon soveltuvuus on sisällytetty kommentit, jotka kuvastavat harjoitusmateriaalin soveltuvuutta erilaisille käyttäjille sekä esimerkiksi materiaalin kattavuutta tai riittävyyttä käsittelevät huomiot.

Haasteina kommenteista nousi esiin joidenkin osioiden vaativuus tietoteknisen osaamisen kannalta. Vastaavasti kommenteissa nostettiin esille suositus (tarve) aloittelijoille soveltuvamman toiminnallisen sisällön lisäämiselle, jotta harjoituskokonaisuus olisi paremmin laajemman käyttäjäkunnan hyödynnettävissä. Esimerkkejä näistä haastavuutta kuvaavista kommenteista on esitetty alla.

-- puheesta on tulkittavissa, että osion soveltuvuus henkilöille, joilla ei ole vahvaa osaamista tietotekniikasta entuudestaan on heikko”

Arvioijalla oli osiossa merkittäviä teknisiä haasteita, jotka johtivat turhautumisiin.

-- puhuja nostaa esille tarpeen aloittelijoille soveltuvamman toiminnallisen sisällön lisäämisen, jotta harjoitus olisi soveltuvampi laajemmalle yleisölle.

Toisaalta kommentteista nousee esille monia kehitysehdotuksia koettujen haasteiden ratkaisemiseksi. Näissä kommentteissa keskityttiin erityisesti yksinkertaisemman lisämateriaalin tarjoamiseen sekä tosielämän kontekstin selkeämpään kuvaamiseen. Muutama esimerkki näistä kommentteista on esitetty alla.

-- tätä haastetta voisi kehittää tarjoamalla yksinkertaistettuja selityksiä sekä laajempaa lisämateriaalia tietyistä osa-alueista.

Myös laajemman tosielämän kontekstin avaaminen voisi tukea yleistä ymmärryksen kehittymistä.

Toisaalta koetuista haasteista huolimatta on kommentteista tulkittavissa, että harjoituskokonaisuus on yleisesti koettu hyväksi sekä kehittäväksi.

Koetuista haasteista huolimatta arvioija pitää kokemustaan positiivisena, vaikka harjoitusosio olikin hänelle hyvin aikaa vievä sekä haastava

Yleisesti arvioija toteaa, että tietoturvan harjoittelu voi olla haasteellista sekä aikaa vievää, mutta samalla hyvin oleellinen osa vahvistamassa teoreettisen tiedon ja käytännön taitojen yhdistämistä

Opitun soveltamista käsittelevät kommentit on puolestaan luokiteltu erilaisten monipuolisuutta, laaja-alaisuutta sekä yleisesti soveltamista tai linkittämistä laajempaan kokonaisuuteen tai käytännön elämään kuvaaviin kommentteihin. Yleisenä laajaa sovellettavuutta kuvaavana kommenttina voidaan nostaa esimerkiksi

-- sovellettavissa todellisen maailman tilanteisiin, sillä siinä yhdistyvät todellisuutta mukailevat simulaatiot sekä käytännön harjoittelu erilaisin soveltavien harjoitusten kautta.

Vastaavasti moduulin monipuolisuutta sekä teoreettisen ymmärryksen ja käytännön tekemisen yhteispeliä kuvaavia kommentteja nousee tekstistä useita.

Esimerkkejä näistä on valikoitu alle.

-- yhdistävän hyvin teoreettinen ymmärrys käytännön sovellutuksiin sekä näiden kautta tosielämän tietoturva-asteisiin.

Moduulissa yhdistyvät käytännön työkalujen käyttö sekä yleinen hyökkäävän sekä puolustavan tietoturvan yhteispeli.

Harjoitusten kuvataan jopa kehittävän ymmärrystä tietoturvallisuuden pohjimmaisten haasteiden ja prosessien osalta

Moduulin arvioidaan myös kykenevän hyvin luomaan realistinen kokonaiskuva käytännön tieturva-asteista sekä niiden käsittelemisestä organisaatiolle järkevällä tavalla varsinkin parhaiden käytäntöiden esittelyn ja käsittelyn kautta

Lisäksi tekstistä nousee esille useita kommentteja, joilla viitataan tietoturvatiETOisuuden parantumiseen sekä yleiseen varautumiseen ja kokonaispuolustuksen kehittymiseen. Muutamia esimerkkejä näistä on valikoitu alle.

-- moduuli parantaa tietoturvatiETOisuuden kehittymistä monipuolisuudellaan sekä käytännön esimerkkien kautta.

-- puhuja esittää, että monipuolinen tietoturvakoulutus soveltuu hyvin tietoturvatiETOisuuden ja yleisen varautumisen edistämiseen.

-- murtautumistestauksen peruseriaatteita, kuten viitekehyksiä ja metodeja, sekä yleisesti murtautumistestaajan roolia osana kokonaispuolustusta.

Puhuja esittää näkemyksen, että käytännön harjoitteiden kautta lisääntyy yleinen tiedostaminen ja valmius tietoturva-asioihin/-poikkeamiin

Toisaalta teemaan soveltaminen sisältyi myös materiaalin ja harjoitusten kehittämiseen viittaavia kommentteja. Näiden kautta esitettiin, että sovellettavuus parantuisi, kun tiettyjen asioiden osalta materiaalia kehitettäisiin eteenpäin. Eri-tyisesti näissä korostui laajemman kokonaisuuden ymmärtämiseen ja opittujen

taitojen nivoutumista yhteen laajemmin sekä puolustautumiseen opittujen tekniikoiden varalta. Esimerkkejä näistä kommentteista on esitetty alla.

-- parempiin tuloksiin pääsemiseksi ehdotetaan, että harjoittelun tulisi tasapainottaa paremmin teknisten taitojen linkittymistä laajempaan kokonaisuuteen, kuten organisatorisen tason vaikutuksia poikkeamatilanteissa sekä linkittymistä turvallisuusstrategiaan.

-- materiaali voisi käsitellä laajemmin kuinka esitetyn kaltaisia heikkouksia/hyökkäyksiä vastaan puolustaudutaan.

Kolmantena suurempana teemana materiaalista tunnistettiin käytännön tekemistä ja tosielämän käyttöä kuvailevat kommentit. Kommenteissa korostuivat positiiviset kokemukset käytännön harjoitteista, sekä vahva usko käytännön harjoitteiden myötä parantuvasta tietoturvatietoisuudesta sekä yleisestä tietoturvasta. Esimerkkejä näistä kommentteista on poimittu alle.

Myös tosielämää simuloivien harjoitusten voidaan ajatella tukevan yleistä tietoturvatietoisuuden kehittymistä

Myös käytännönläheiset tosielämän esimerkit nostetaan tekstissä esille hyvänä valmentavana esimerkkinä tosielämän tietoturvahaasteisiin valmistautumisessa

Käytännön elämää simuloivien harjoitusten todetaan olevan avainasemassa harjoituksen tehokkuudessa.

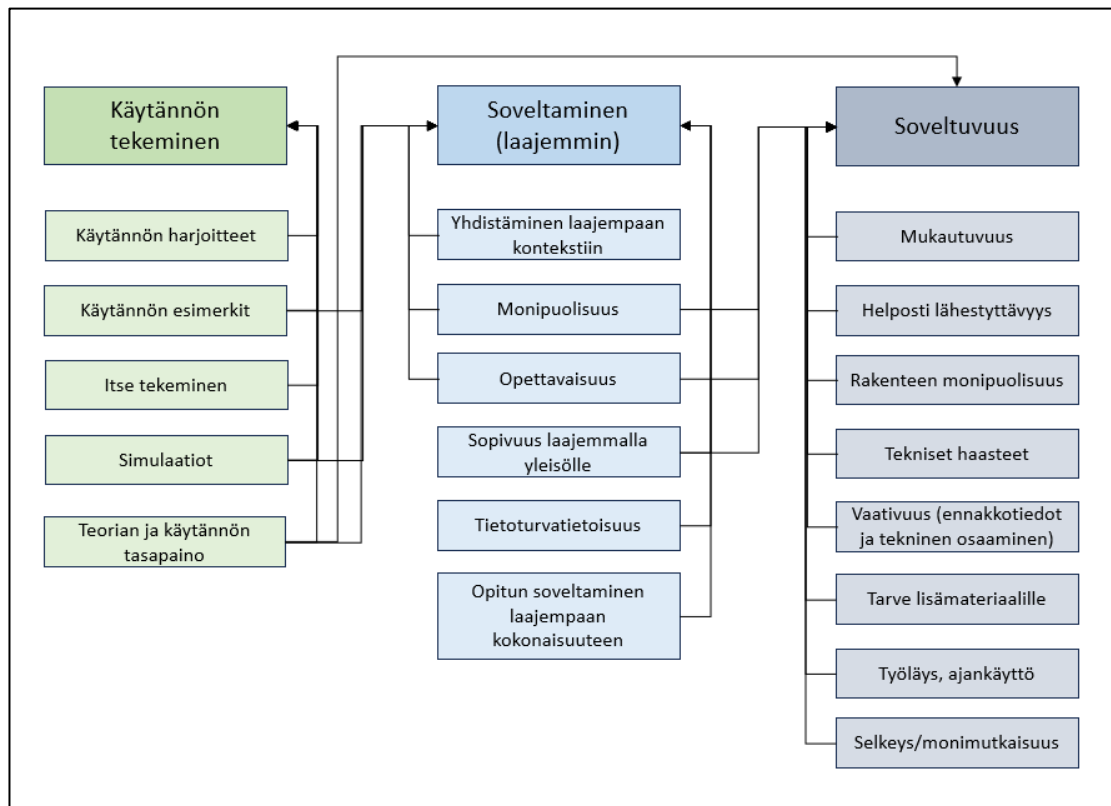
Puhuja esittää Network Security osion tukevan tietoturvatietoisuuden kasvattamista erityisesti erilaisten käytännön taitojen kehittämisen sekä työkalujen toiminnan opettelun kautta.

Käytännön harjoitteista arvioija pitää tosielämän esimerkkejä tärkeänä osana moduulia ja arvioi näiden tukevan laajemman organisaatiotason tietoturvan ymmärrystä sekä parantamista

Erytisen positiivisesti puhuja suhtautuu tosielämään tilanteita simuloivien harjoitteiden käytännönläheiseen soveltamiseen

Tietoturvatietoisuuden parantamisen nähden erityisesti syntyvän käytännön harjoitteiden kautta

Reflektioivan tutkimuksen temaattisen koodauksen ja teemoituksen suhdetta on kuvattu alla (Kuva 8).



Kuva 8. Reflektioanalyysin temaattinen kartta, muiden kokemukset

Muiden kokemusten perusteella tehdyssä analyysissä korostuu erityisesti positiivisuus liittyen harjoittelun soveltuvuuteen tietoturvallisuuden kehittämiseksi sekä yleisesti positiivisuus liittyen käytännön tekemiseen. Toisaalta näihin kommentteihin on hyvä suhtautua enemmän varauksella, sillä puhujan motivaatiovaikuttimet positiivisen mielikuvan antamiselle tai tekoälypurin syötteen vaikutus kommenttien tulkintaan voivat vaikuttaa merkittävästikin kommenttien sävyyn.

Käyttäjien kokemusten arvioissa korostuu, kuten reflektioanalyysissäkin, positiiviset kokemukset käytännön harjoitteista sekä tulkinta opitun soveltamisesta laajemmin. Toisaalta myös työläys, monimutkaisuus tai haastavuus, sekä lisämateriaalien tarve näyttäytyy myös näissä kommentteissa.

Yleisesti on tulkittavissa, että muiden käyttäjien kokemukset vertautuvat kohtalaisen hyvin tutkijan omaan kokemukseen. Näin voidaankin yleisesti tulkita vertailututkimuksen tukevan käyttäjätutkimuksen tuloksia.

4.3 Tulosten tulkinta

Tämän tutkimuksen tarkoituksena oli tutkija murtautumistestauksen harjoittelun soveltuvuutta tietoturvaluotteluun lisäämiseksi. Kun tietoturvaluotteluun lisäämistä käsitellään prosessina Tsohou ym. (2008) mukaisesti, joka pyrkii muuttamaan mm. näkemyksiä, arvoja, asenteita sekä työskentelytapoja tukemaan paremmin tietoturvaluottelua käytänteitä, on tulkittavissa kokemusten perusteella, että tutkittu harjoittelumuoto voi muuttaa harjoittelijoiden ymmärrystä sekä mahdollisesti myös auttaa muovaamaan käytäntöjä kohti tietoturvaluottelua tapaa. Yleisesti tehdyt analyysit tukevat Gjersten ym. (2017) esittämää näkemystä pelillisten harjoitusten positiivisesta vaikutuksesta nopeampaan oppimiseen, laajempaan ymmärrykseen sekä laajempaan osaamiseen yleisistä tietoturvaluottelukonsepteista.

Toisaalta, jos organisaatioiden tietoturvaluotteluun lisäämisen peruseräteenä pidetään kaikkien työntekijöiden kouluttamista tietoturvaluottelun varalle on tulkittavissa, että tutkittu harjoittelumuoto ei yksinään sovi tähän tarkoitukseen. Tämä tulkinta on johdettavissa siitä, että harjoittelutapa on hyvin työläs eikä siten organisaation näkökulmasta kustannustehokas. Lisäksi tehdyt harjoitteet vaativat merkittävää ennako-osaaamista aihepiiriä tukevista seikoista, joten menetelmä ei ole kaikille soveltuva.

Tulosten perusteella on tulkittavissa, että käyttäjät pitivät materiaalia sekä harjoittelutapaa yleisesti kiinnostavana, sekä itselleen sopivana. Tämän voidaan tulkita viittaavan siihen, että menetelmä voisi olla yksi keino Bada ym. (2019) esittämän merkittävimmän tietoturvaluotteluun lisäämisen esteen, kiinnostavien ja sopivien koulutusmateriaalien puuttumisen, ylittämiseen.

Kommenttien perusteella ei ole selvää, muuttiko tehty harjoittelu asenteita suosivimmiksi muilla menetelmillä toteutettuja koulutuksia kohtaan, vaikka näin on lähdekirjallisuudessa (Ghazvini & Shukur, 2018) esitetty. Toisaalta kommentteista ei ole myöskään tulkittavissa vastakkaista näkökantaa, joten on luontevaa jättää lähdekirjallisuuden esittämän positiivinen vaikutus oletetuksi vaikutukseksi.

Yleisesti onkin johdettavissa näkemys tietoturvatietoisuuden edistämiseen soveltuvasta koulutuskokonaisuudesta sellaiseksi, jossa murtautumistestauksen harjoittelu on osa koulutustarjontaa, mutta jota käytetään vain rajatuissa tapauksissa vastaamaan kompleksisuushaasteeseen tai syventämään erityisosaamista aihepiireistä, jotka jo entuudestaan vaativat syvällistä tietotekniikan ymmärrystä. Esimerkiksi erilaiset tietoiskut, ryhmäkeskustelut sekä muut vähäistä suoritusaikaa vaativat sekä laajalle yleisölle helposti jaettavat menetelmät säilyttävät näin paikkansa kaikkein tärkeimpinä keinoina tietoturvatietoisuuden edistämiseen.

5 Yhteenveto ja keskustelu

Tämän työn tarkoituksena oli tutkia murtautumistestauksen harjoittelun soveltuvuutta tietoturvallisuustietoisuuden lisäämiseksi sekä tarkastella murtautumistestausta yleisesti osana tietoturvallisuuden kokonaisuutta. Työssä koottiin kirjallisuuskatsauksen avulla yleiskuva murtautumistestauksesta sekä arvioitiin käyttäjätutkimuksen avulla murtautumistestausalustalla toteutettavan harjoittelun soveltuvuutta tietoturvallisuuden kehittämiseksi.

Tutkimuksen tulosten perusteella esitetään, että murtautumistestauksen harjoittelu on soveltuva keino tietoturvatietoisuuden lisäämiseksi, sillä sen avulla voidaan muuttaa mm. näkemyksiä, asenteita sekä työskentelytapoja tukemaan paremmin tietoturvallisia käytänteitä. Lisäksi esitetään, että kirjallisuudessa esitetyt näkemyksen pelillisten harjoitteiden positiivisesta vaikutuksesta oppimisnopeuteen sekä laajemmin ymmärrykseen sekä osaamiseen yleisistä tietoturvakonsepteista pätevät.

Toisaalta tutkimus osoittaa, että tutkittu harjoittelumuoto tarvitsee tuekseen muitakin opetusmuotoja tietoturvatietoisuuden parantamiseksi organisaatioissa. Eri-tyisesti tutkitun menetelmän työläys sekä vaatima ennakkotiedon määrä rajavat harjoittelumenetelmän kustannustehokasta käyttöä.

Hyvin kohdennettuna voidaan menetelmän tulkita sopivan tietyille käyttäjäryhmälle. Eri-tyisesti menetelmää voidaan pitää keinona vastaamaan yhteen tietoturvatietoisuuden lisäämisen merkittävimpään haasteeseen, kiinnostavien ja käyttäjälle sopivien koulutusmateriaalien puuttumiseen, rajatun käyttäjäryhmän osalta.

Tutkimus esittää, että tutkittu menetelmä on soveltuva keino tietoturvatietoisuuden edistämiseen rajatuissa tapauksissa ja vastaamaan ns. kompleksisuus-haasteeseen sekä syventämään erityisosaamista aihepiireistä käyttäjille, joilla jo entuudestaan on syvä tietotekninen ymmärrys. Muut keinot, kuten tietois-
kut, ryhmäkeskustelujen sekä muut vähäistä suoritusaikaa vaativat sekä laajalle yleisölle helposti jaettavissa olevat menetelmät esitetään kuitenkin parempina keinoina laajamittaiseen tietoturvatietoisuuden lisäämiseen.

Tutkimuksen perusteella voidaan menetelmää suositella yhdeksi keinoksi osana kokonaisvaltaista koulutussuunnitelmaa, joka muokataan käyttäjäkohtaisesti tukemaan kunkin henkilön ominaisuuksia sekä tarpeita.

Tuloksien soveltamisessa käytäntöön tulee huomioida myös tutkimuksen heikoudet sekä puutteet. On hyvä huomioida, että tässä työssä tutkittiin vain yhtä alustaa ja tästäkin vain yhtä oppimispolkua, joten tutkimustulosten yleistettävyyteen on hyvä suhtautua varauksella. Toisaalta yhtenä merkittävimmistä vaikutuksista toteutettuun tutkimukseen on tutkijan subjektiivinen näkökanta, mikä vaikuttaa vahvasti tutkijan kokemuksiin sekä tutkijan tulkintoihin analysoidun aineiston osalta. Vaikka tässä tutkimuksessa subjektiivisen harhan vaikutusta on pyritty lieventämään tekoälyavusteisella vertailututkimuksella, ovat myös näissä aineistoissa esiintyvien käyttäjien kokemukset vaikuttaneita heidän taustoistaan,

arvomaailmastaan sekä yleisesti tietoteknisestä osaamisestaan. Vastaavasti toteutettuun vertailututkimukseen vaikuttaa merkittävästi käytetyn mallin ominaisuudet sekä mallille annettu syöte. Vaikka suurenkin aineiston käsittely on tällaisella mallilla tehokasta, on mallin kyky tehdä tulkintoja rajallinen. Yleisesti tällainen malli toimii nk. mustana laatikkona eli käyttäjälle ei ole selvää, miten malli päätyy esittämiinsä päätelmiin. On myös hyvä tiedostaa, että tällainen malli voi tuottaa epätarkkaa tai jopa virheellistä informaatiota, joten on hyvä tiedostaa tällainen tekoälyn hallusinaation mahdollisuus.

Aihepiirin jatkotutkimuskohteiksi suositellaan rinnakkaisanalyysiä käyttäjän ja tekoälyavusteisen työkalun kesken samasta aineistosta, jolla voitaisiin varmentaa tekoälyapurin toiminnan luotettavuutta. Lisäksi refleктоiva käyttäjätutkimus olisi hyvä laajentaa kattamaan useamman käyttäjän kokemukset. Vastaavasti erilaisia murtautumistestausalustoja ja eri harjoittelukokonaisuuksia tulisi myös tutkia, jotta saataisiin muodostettua parempi kuva murtautumistestauksen harjoittelusta yleisemmin.

Lähteet

- Abawajy, J., 2014. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33
- Aiyanyo, I.D., Samuel, H. and Lim, H., 2020. A systematic review of defensive and offensive cybersecurity with machine learning. *Applied Sciences*, 10(17), p.5811.
- Alotaibi, M., & Alfehaid, W. (2018). Information security awareness: A review of methods, challenges and solutions. *Proceedings of the ICITST-WorldCIS-WCST-WCICSS-2018*, Cambridge, UK, 10, 13.
- Alshaikh, M., Maynard, S.B., Ahmad, A. and Chang, S., 2018. An exploratory study of current information security training and awareness practices in organizations.
- Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. *arXiv preprint arXiv:1901.02672*.
- Tidy, J. 2022. BBC artikkeli. Police launch homicide inquiry after German hospital hack. Viitattu 1.10.2024. <https://www.bbc.com/news/technology-54204356>
- Bing, C. and Kelly, S., 2021. Cyber attack shuts down US fuel pipeline 'juggular,' Biden briefed. *Reuters*. Accessed, pp.05-25.
- Bresz, F. P. (2004). People--Often the Weakest Link in Security, But One of the Best Places to Start. *Journal of health care compliance*, 6(4).
- Capano, D. E. 2023. Throwback Attack: How NotPetya accidentally took down global shipping giant Maersk: Do you debate risks vs. cost of cybersecurity technologies, processes and training? Maersk estimated NotPetya costs at \$250-300 million. *Control Engineering*, 704, 39-42

Collins, G. 2023. Video. I Played HackTheBox For 30 Days - Here's What I Learned. Viitattu 1.10.2024. <https://www.youtube.com/watch?v=bPv5pb7AcYs>

CyberEyes, 2022. Video. TryHackme! Intro to Offensive Security Walkthrough. Viitattu 1.10.2024. <https://www.youtube.com/watch?v=rcBdr-SeZ8tg&list=PLNK290KWIoDY4MLS-rQCJyW9pKL9gb6Sx>

DeValk, K., Gwilliam, M., Hanson T., Harrity, M., and Mazurek, M. "Industry Perspectives on Offensive. Security Tooling". In: SOUPS WSIW. 2022

DVV 2024. Verkkosivu, viitattu 27.9.2024. <https://dvv.fi/-/digiturvabarometri-verkkorikollisuus-on-laskenut-luottamusta-digimaail-maan-mutta-siita-huolimatta-siedamme-hyvin-muuttunutta-uhkatilannetta>

EC-Council, 2022. Verkkosivu. Understanding the Five Phases of the Penetration Testing Process. Viitattu 1.10.2024. <https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/>

Espinosa, L. 2023. Is Tryhackme worth it? I finished one of their courses and this is my honest opinion.. Viitattu 1.10.2024. <https://www.linkedin.com/pulse/tryhackme-worth-i-finished-one-courses-my-honest-espinosa-r-ruzyc>

Fireshark, 2023. Video. #TryHackMe | Introduction to Cybersecurity. Viitattu 1.10.2024. <https://www.youtube.com/watch?v=je2sDfHYtH8>

Rocha Flores, Waldo & Ekstedt, Mathias. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*. 59. 10.1016/j.cose.2016.01.004.

Ghazvini, Arash & Shukur, Zarina. (2018). A Serious Game for Healthcare Industry: Information Security Awareness Training Program for Hospital Universiti Kebangsaan Malaysia. *International Journal of Advanced Computer Science and Applications*. 9. 10.14569/IJACSA.2018.090932.

Gjertsen, Eyvind & Gjære, Erlend Andreas & Bartnes, Maria & Rocha Flores, Waldo. (2017). Gamification of Information Security Awareness and Training. 59-70. 10.5220/0006128500590070.

Huntley, S. (2023). Fog of war: how the Ukraine conflict transformed the cyber threat landscape. Google Threat Analysis Group, 16.

Hadam, M. 2022. Video. The Complete Windows Privilege Escalation Course | TryHackMe Windows Privesc | OSCP. Viitattu 1.10.2024. https://www.youtube.com/watch?v=k_99-dXtdpc

Haque, M. A., & Li, S. (2024). Exploring chatgpt and its impact on society. *AI and Ethics*, 1-13.)

Hamdan, M. 2021. Video. The Complete Linux Privilege Escalation Course | TryHackMe Junior Penetration Tester | OSCP. Viitattu 1.10.2024. <https://www.youtube.com/watch?v=7WQndt-1WzE>

Harper, A., Linn, R., Sims, S., Baucom, M., Fernandez, D., Tejada, H. and Frost, M., 2022. Gray hat hacking: the ethical hacker's handbook. McGraw-Hill Education.

Hart, S., Margheri, A., Paci, F. and Sassone, V., 2020. Riskio: A serious game for cyber security awareness and education. *Computers & Security*, 95, p.101827.)

Hartley, M. E. (2022). Access Denied: The Dangers of Ransomware's Unchecked Attack on the Agriculture Industry. *Drake J. Agric. L.*, 27, 457.

Hon, K. 2023. Jr Penetration Tester Learning Path ~ TryHackMe. Viitattu 1.10.2024. <https://medium.com/@thamkeyhon/jr-penetration-tester-learning-path-tryhackme-6432c415fbc9>

IBM, 2022. Mansfield-Devine, S., 2022. IBM: Cost of a Data Breach.

IBM, 2023. Verkkosivu. The penetration testing process. Viitattu 1.10.2024.
<https://www.ibm.com/topics/penetration-testing>

ICO n.d. Verkkosivu, viitattu 27.9.2024. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/ransomware-and-data-protection-compliance/>

InfoSec, P. 2023. Video. TryHackMe VS HackTheBox - Which One Is Better For YOU in 2023-2024 - InfoSec Pat. Viitattu 1.10.2024.
<https://www.youtube.com/watch?v=CvGiBc7eeLA>

Jelo, M. and Helebrandt, P., 2022, October. Gamification of cyber ranges in cybersecurity education. In 2022 20th International Conference on Emerging eLearning Technologies and Applications (ICETA) (pp. 280-285). IEEE.

Joensuu, T., 2023. Ukrainan sodan vaikutukset organisaatioiden kyberturvallisuuteen Suomessa.

Karagiannis, S., Papaioannou, T., Magkos, E. and Tsohou, A., 2020. Game-Based Information Security/Privacy Education and Awareness: Theory and Practice. In Information Systems: 17th European, Mediterranean, and Middle Eastern Conference, EMCIS 2020, Dubai, United Arab Emirates, November 25–26, 2020, Proceedings 17 (pp. 509-525). Springer International Publishing.

Khan, B., Alghathbar, K.S., Nabi, S.I. and Khan, M.K., 2011. Effectiveness of information security awareness methods based on psychological theories. African journal of business management, 5(26), p.10862.

Khando, K., Gao, S., Islam, S.M. and Salman, A., 2021. Enhancing employees information security awareness in private and public organisations: A systematic literature review. Computers & security, 106, p.102267.

Kim, K., Alfouzan, F.A. and Kim, H., 2021. Cyber-attack scoring model based on the offensive cybersecurity framework. Applied Sciences, 11(16), p.7738.

Kortesoja, M. 2022. Tapaus Vastaamo: Symptomaattinen luenta potilastietosuojan murtumisen yhteiskunnallisista syistä ja seurauksista.

Kulkarni, A., Wang, Y., Gopinath, M., Sobien, D., Rahman, A., & Batarseh, F. A. (2024). A Review of Cybersecurity Incidents in the Food and Agriculture Sector. arXiv preprint arXiv:2403.08036.

Mäki, M. L. (2022). "Tämä koskettaa meitä kaikkia": Vastaamon tietomurto ja luottamuksen menetys.

Marjamaa, M., & Sinisalo, R. (2022). Kirjallisuuskatsauksen ohjaus-perustana tutkimuskysymys ja ohjaushaastattelu. Kreodi-ammattikorkeakoulukirjastojen verkkolehti. Viitattu, 21, 2024.

NIST 800-155. Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). Technical guide to information security testing and assessment. NIST Special Publication, 800(115), 2-25.

Ortlipp, M. (2008). Keeping and using reflective journals in the qualitative research process. *The qualitative report*, 13(4), 695-705.

Ortiz-Garces, I., Gutierrez, R., Guerra, D., Sanchez-Viteri, S., & Villegas-Ch, W. 2023. Development of a Platform for Learning Cybersecurity Using Capturing the Flag Competitions. *Electronics*, 127, 1753.

Paavola, J. (2014) *Näkökulmia tietoturvaan 2*. Turun ammattikorkeakoulu, Turku 2014. ISBN 978-952-216-444-5.

Palaez, R. 2022. Video. SSRF - TryHackMe - [Jr Penetration Tester Path] - Introduction to Web Hacking. Viitattu 1.10.2024. https://www.youtube.com/watch?v=X_NhSepLOjM

Palmer, C.C., 2001. Ethical hacking. *IBM Systems Journal*, 40(3), pp.769-780.

PTES, 2014. Verkkosivu. Penetration Testing Execution Standard. Viitattu 1.10.2024. <http://www.pentest-standard.org/>

Rautakoura, J., 2023. Venäjän hyökkäys Ukrainaan ja sen vaikutus Suomen kyberturvallisuuteen.

Reddit-keskustelu. 2022. Jr Pen Tester vs Offensive Pen Testing learning path. Viitattu 1.10.2024. https://www.reddit.com/r/tryhackme/comments/vbr4m9/jr_pen_tester_vs_offensive_pen_testing_learning/?rdt=44195

RIKUteema, 2/2022. Verkkosivu, viitattu 27.9.2024. <https://www.riku.fi/rikosuhripaivystys/rikuteema/laajat-rikostapahtumat/kaksi-vuotta-vastaamon-tietomurosta-nain-yksi-rikos-muutti-yhteiskuntaa/>

Rosen B, 2023j. Video. Nmap Basic Port Scans - TryHackMe Junior Penetration Tester: 5.4. Viitattu 1.10.2024. https://www.youtube.com/watch?v=_UeHx3XH5A

Rosen, B. 2023a. Video. Pentesting Fundamentals - TryHackMe Junior Penetration Tester: 2.1. Viitattu 1.10.2024. <https://www.youtube.com/watch?v=6puBsskqVvQ>

Rosen, B. 2023b. Video. Burp Suite: The Basics - TryHackMe Junior Penetration Tester 4.1. Viitattu 1.10.2024. <https://www.youtube.com/watch?v=HZqCeVD1Hew>

Rosen, B. 2023c. Video. Burp Suite: Repeater - TryHackMe Junior Penetration Tester 4.2. Viitattu 1.10.2024. <https://www.youtube.com/watch?v=dJy0dVIWGtl>

Rosen, B. 2023d. Video. Burp Suite: Intruder - TryHackMe Junior Penetration Tester 4.3. Viitattu 1.10.2024. <https://www.youtube.com/watch?v=eaOk-N1UQuU>

Rosen, B. 2023e. Video. Burp Suite: Other Modules - TryHackMe Junior Penetration Tester 4.4. Viitattu 1.10.2024. <https://www.youtube.com/watch?v=NCy-mUobjtSc>

Rosen, B. 2023f. Video. Burp Suite: Extender - TryHackMe Junior Penetration Tester 4.5. Viitattu 1.10.2024. <https://www.youtube.com/watch?v=K6IXYPUH-hdQ>

Rosen, B. 2023g. Video. Passive Reconnaissance - TryHackMe Junior Penetration Tester: 5.1. Viitattu 1.10.2024. <https://www.youtube.com/watch?v=fpl30-rnp-o>

Rosen, B. 2023h. Video. Active Reconnaissance - TryHackMe Junior Penetration Tester: 5.2. Viitattu 1.10.2024. <https://www.youtube.com/watch?v=nBboVL-Wahol>

Rosen, B. 2023i. Video. Nmap Live Host Discovery - TryHackMe Junior Penetration Tester: 5.3. Viitattu 1.10.2024. <https://www.youtube.com/watch?v=ZsEejncp0bc>

Rosen, B. 2023k. Video. Nmap Advanced Port Scans - TryHackMe Junior Penetration Tester: 5.5. Viitattu 1.10.2024. <https://www.youtube.com/watch?v=Ab-T9GA8RO8>

Rosen, B. 2023l. Video. Nmap Post Port Scans - TryHackMe Junior Penetration Tester: 5.6. Viitattu 1.10.2024. <https://www.youtube.com/watch?v=Lc5-bMHsSr8>

Rosen, B. 2023m. Video. Protocols and Servers - TryHackMe Junior Penetration Tester: 5.7. Viitattu 1.10.2024. https://www.youtube.com/watch?v=rb-TXIIH_Io

Rosen, B. 2023n. Video. Protocols and Servers 2 - TryHackMe Junior Penetration Tester: 5.8. Viitattu 1.10.2024. https://www.youtube.com/watch?v=5d_E9aayByo

Rosen, B. 2023o. Video. Net Sec Challenge - TryHackMe Junior Penetration Tester: 5.9. Viitattu 1.10.2024. https://www.youtube.com/watch?v=_s2oDTnsb7M

Rosen, B. 2023p. Video. Vulnerabilities 101 - TryHackMe Junior Penetration Tester: 6.1. Viitattu 1.10.2024. <https://www.youtube.com/watch?v=pTq-T2NO474>

Rosen, B. 2023q. Video. Exploit Vulnerabilities - TryHackMe Junior Penetration Tester: 6.2. Viitattu 1.10.2024. <https://www.youtube.com/watch?v=xzOH-kNyV6xQ>

Rosen, B. 2023r. Video. Vulnerability Capstone - TryHackMe Junior Penetration Tester: 6.3. Viitattu 1.10.2024. <https://www.youtube.com/watch?v=LE5NLCnz0Kw>

Rosen, B. 2023s. Video. Metasploit: Introduction - TryHackMe Junior Penetration Tester: 7.1. Viitattu 1.10.2024. <https://www.youtube.com/watch?v=S7cY-qRAavDk>

Rosen, B. 2023t. Video. Metasploit: Exploitation - TryHackMe Junior Penetration Tester: 7.2 Viitattu 1.10.2024. <https://www.youtube.com/watch?v=wJ7ot-bQrrtQ>

Rosen, B. 2023u. Video. Metasploit: Meterpreter - TryHackMe Junior Penetration Tester: 7.3. Viitattu 1.10.2024. <https://www.youtube.com/watch?v=96V-nwvtaks>

Rosen, B. 2023v. Video. What the Shell? - TryHackMe Junior Penetration Tester: 8.1. Viitattu 1.10.2024. <https://www.youtube.com/watch?v=zc5Z6C2zmNA>

Salminen, A., 2011. Mikä kirjallisuuskatsaus?: Johdatus kirjallisuuskatsauksen tyypeihin ja hallintotieteellisiin sovelluksiin.

Sanastokeskus, 2015.: <https://sanastokeskus.fi/tsk/fi/termitalkoot>

Shaunna's Workshop. 2022. Video. Quick Recap! TryHackMe "Pentesting Fundamentals". Viitattu 1.10.2024. https://www.youtube.com/watch?v=iN33tMmpq7c&list=PLJ0dPsRB5byURFsfKUTmkle3P9WJ_3Ha&index=6

Švábenský, V., Čeleda, P., Vykopal, J., & Brišáková, S. 2021. Cybersecurity knowledge and skills taught in capture the flag challenges. *Computers & Security*, 102, 102154.

Traficom 2022. Verkkosivu, viitattu 27.9.2024. <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberympariston-uhkataso-noussut-aktiviteetti-suomeakin-kohtaan-lisaantynyt>

Traficom 2023a: Näin pidät huolta tietoturvasta kotona ja työpaikalla | Kyberturvallisuuskeskus

Traficom 2023b: <https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva>

Tsohou, A., Karyda, M. and Kokolakis, S., 2015. Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & security*, 52, pp.128-141.

Tsohou, A., Kokolakis, S., Karyda, M. and Kiountouzis, E., 2008. Investigating information security awareness: research and practice

TurunYliopisto, 2024. ChatGPT ja muut tukiälysovellukset. Kirjaston teko-älyopas. Viitattu 25.10.2024. <https://utuguides.fi/c.php?g=709314&p=5116862>.

Turobov, A., Coyle, D., & Harding, V. (2024). Using ChatGPT for thematic analysis. arXiv preprint arXiv:2405.08828.

Vegesna, V. V. (2023). Utilising VAPT Technologies (Vulnerability Assessment & Penetration Testing) as a Method for Actively Preventing Cyberattacks. International Journal of Management, Technology and Engineering, 12.

WEF 2024. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf.

Washington Post, 2022. WP Creative Group. Cyber threats, real-world consequences. Viitattu 1.10.2024. <https://www.washingtonpost.com/creativegroup/ibm/cyber-threats-real-world-consequences/>

Zhang, H., Wu, C., Xie, J., Kim, C., & Carroll, J. M. (2023a). QualiGPT: GPT as an easy-to-use tool for qualitative coding. arXiv preprint arXiv:2310.07061.

Zhang, H., Wu, C., Xie, J., Lyu, Y., Cai, J., & Carroll, J. M. (2023b). Redefining qualitative analysis in the AI era: Utilizing ChatGPT for efficient thematic analysis. arXiv preprint arXiv:2309.10771.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F. and Basim, H.N., 2022. Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62(1), pp.82-97.

Liitteet

Liite 1. Esimerkkisyöte (ChatGPT)

Your role is to be an academic expert in Qualitative Thematic Analysis, specializing in helping researchers in the fields of information security, cyber security, security awareness and organizational training. You will assist in qualitative text analysis coding data, offering guidance on identifying themes and interpreting results. You should emphasize accuracy, relevance, and depth in analysis while avoiding giving personal opinions or engaging in debates. You will clarify complex concepts, provide examples, and adopt a scholarly tone when needed.

you will analyze the following text for speakers opinion or view, in relation to Applicability of conducted training as a tool for increasing cyber security awareness as well as the applicability of the tested program for this purpose.

[Text to be inserted here]

Liite 2. Esimerkkituloste (ChatGPT)

To analyze the given text in relation to the applicability of conducted training as a tool for increasing cyber security awareness, we should focus on extracting and evaluating the underlying opinions or views expressed regarding the effectiveness of the training program and its relevance to enhancing cyber security awareness. The text is a detailed walkthrough of an exploitation process using specific tools and commands, likely part of a training or educational exercise.

Key Aspects to Analyze:

Applicability of Training Program:

The text appears to be a practical demonstration of using various cyber security tools and techniques, such as exploiting SMB vulnerabilities, interacting with the Meterpreter session, and performing hash dumps.

The instructor emphasizes the practical application of these techniques, suggesting that the training program involves hands-on exercises designed to simulate real-world scenarios. This approach is often effective for increasing cyber security awareness because it provides learners with concrete experience in handling security tools and understanding vulnerabilities.

Effectiveness of the Training:

The text includes praise for the completion of tasks ("nice job guys," "woohoo"), indicating that the training is designed to be engaging and rewarding. This positive reinforcement can enhance the learning experience and make the training more memorable.

There is a focus on detailed procedural knowledge, such as using specific commands and tools, which suggests that the training aims to build a deep understanding of practical cyber security skills.

Relevance to Cyber Security Awareness:

By demonstrating the process of exploiting vulnerabilities and handling sessions, the training helps participants understand the implications of security weaknesses and the methods attackers might use. This knowledge is crucial for improving security awareness.

The inclusion of explanations about hashing vs. encryption and the practical steps to find and analyze files reinforces the relevance of the training in real-world contexts.

Evaluation of Training Program for Increasing Cyber Security Awareness:

The training program, as illustrated in the text, appears to be effective in terms of practical application and engagement. It provides learners with hands-on experience and detailed instructions, which can significantly enhance their understanding of cyber security concepts and practices.

However, the text does not provide direct feedback on the training's effectiveness or applicability beyond the demonstration itself. For a comprehensive evaluation, feedback from participants and assessment of their performance in applying these skills in real-world scenarios would be necessary.

Summary:

The text suggests that the training program is well-designed to increase cyber security awareness by providing practical, hands-on experience with cyber security tools and techniques. The positive reinforcement and detailed procedural knowledge contribute to a comprehensive learning experience. However, a full assessment of the training's applicability and effectiveness would require additional feedback from participants and evaluation of their ability to apply the skills learned in real-world contexts.